United States General Accounting Office

GAO

Report to Congressional Requesters

June 2004

MARITIME SECURITY

Substantial Work Remains to Translate New Planning Requirements into Effective Port Security

On July 2, 2004, the PDF file was revised to show the correct location of ports in Alaska, Hawaii, and Texas in Figure 1 on page 9

G A O

Accountability ⋆ Integrity ⋆ Reliability

GAO-04-838

June 2004

MARITIME SECURITY

Substantial Work Remains to Translate New Planning Requirements into Effective Port Security

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-838, a report to congressional requesters

Why GAO Did This Study

The Maritime Transportation Security Act of 2002, as implemented by the Coast Guard, calls for owners and operators of about 3,150 port facilities (such as shipping terminals or factories with hazardous materials) and about 9,200 vessels (such as cargo ships, ferries, and tugs and barges) to develop and implement security plans by July 1, 2004. The Coast Guard intends to conduct on-site compliance inspections of all facilities by January 1, 2005, and all vessels by July 1, 2005, to ensure plans are adequately implemented. The Coast Guard estimated the act's security improvements would cost $7.3 billion over 10 years—most of it borne by facility and vessel owners and operators. GAO was asked to assess (1) the progress towards developing, reviewing, and approving plans by July 1, 2004, (2) the Coast Guard's monitoring and oversight strategy for ensuring that plans are implemented, and (3) the accuracy of the Coast Guard's cost estimate.

What GAO Recommends

GAO recommends that the Coast Guard evaluate its initial compliance efforts and use them to strengthen the compliance process for its long-term strategy. As part of this strategy, the Coast Guard should clearly define inspector qualifications and consider including unscheduled and unannounced inspections and covert testing. The Coast Guard agreed.

www.gao.gov/cgi-bin/getrpt?GAO-04-838.

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

Owners and operators have made progress in developing security plans for their port facilities and vessels. However, the extent to which the Coast Guard will have reviewed and approved the approximately 12,300 individual plans by July 1, 2004, varies considerably. About 5,900 plans were being developed under an option allowing owners and operators to self-certify that they would develop and implement plans by July 1, using industry-developed, Coast Guard-approved standards and templates. These individual plans will not be reviewed before July 1 unless owners or operators choose to submit them for review. The remaining 6,400 plans went through a review process established by the Coast Guard. Every plan required revisions, some of which were significant. As of June 2004—1 month before the deadline for implementation—more than half of the 6,400 plans were still in process. The Coast Guard took steps to speed up the process and to allow facilities and vessels to continue operating with less than full plan approval after July 1, as long as the Coast Guard was satisfied with their progress.

The Coast Guard's strategy for monitoring and overseeing security plan implementation will face numerous challenges. Whether the Coast Guard will be able to conduct timely on-site compliance inspections of all facilities and vessels is uncertain because questions remain about whether the Coast Guard will have enough inspectors; a training program sufficient to overcome major differences in experience levels; and adequate guidance to help inspectors conduct thorough, consistent reviews. Another challenge is to ensure inspections reflect assessments of the normal course of business at facilities and aboard vessels.

The accuracy of the Coast Guard's $7.3 billion estimate for implementing security improvements is likewise uncertain. The estimate, while a good-faith effort on the Coast Guard's part, is based on limited data and on assumptions that are subject to error. The estimate should be viewed more as a rough indicator than a precise measure of costs.

Port facilities pose many security concerns, given their size, accessibility, and attractiveness as terrorist targets. Facilities like these must have a security plan in place by July 1, 2004.

Source: Coast Guard.

Contents

Figures

Abbreviations

AMSC	Area Maritime Security Committee
ASP	Alternative Security Program
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security Code
MARSEC	Maritime Security Condition System
MTSA	Maritime Transportation Security Act
SOLAS	International Convention for Safety of Life at Sea

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

June 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

Since the terrorist attacks of September 11, 2001, the nation's 361 ports have increasingly been viewed as potential targets for future attacks for many reasons. For example, security experts remain concerned about the potential for using the maritime transportation system as a conduit for smuggling weapons of mass destruction or other dangerous materials into the country. Further, cargo and cruise ships present potentially desirable terrorist targets, given the potential for loss of life, ecological destruction, or disruption of commerce. And ports often are not only gateways for the movement of goods, but also industrial hubs and close to population centers, presenting additional opportunities for terrorists bent on urban destruction. Coordinating a security response for this myriad of potential targets is a daunting proposition, in part because so many different stakeholders are involved. These stakeholders include law enforcement and other government agencies at every level (federal, state, and local); vessel owners and operators; railroads; port authorities; factories and other businesses; and people who work in port areas or live nearby. Although perspectives may vary, the specter of further terrorist incidents has led to widespread agreement that port security should be strengthened—and soon.

The Maritime Transportation Security Act (MTSA)[1] contains much of the federal government's approach to addressing these security vulnerabilities. Enacted in November 2002 and largely administered by the United States Coast Guard, an agency within the Department of Homeland Security,

[1]P.L. 107-295, 116 Stat. 2064, 2066 (2002).

MTSA is designed, in part, to help protect the nation's ports and waterways from terrorist attacks through a wide range of security improvements. One of its central maritime transportation security provisions is a requirement that security plans be developed and implemented for specific facilities (such as factories, cargo terminals, and power plants); certain individual cargo and passenger vessels; and entire ports.[2] The basic aim of such plans is to address potential vulnerabilities that could be exploited to kill people, cause environmental damage, or disrupt transportation systems and the economy, by developing measures to mitigate these vulnerabilities. The Coast Guard established regulations determining which facilities and vessels were to be covered by these security planning requirements[3] and consistent with MTSA, set a deadline of July 1, 2004, for facility and vessel owners and operators to operate under an approved or self-certified security plan. Further, the Coast Guard intends to conduct on-site compliance inspections of all facilities by January 1, 2005, and all vessels by July 1, 2005, to ensure that they have satisfactorily implemented their plans. This aggressive timeline for both developing and implementing security plans reflects the seriousness of the port security issue. However, the timeline also creates a substantial and immediate workload for the Coast Guard and for owners and operators who collectively must develop plans for thousands of facilities and vessels. The Coast Guard estimated that the security improvements imposed by these requirements would likely cost port stakeholders $7.3 billion over 10 years—most of it borne by facility and vessel owners and operators.[4]

You asked us to examine the efforts of stakeholders and the Coast Guard in carrying out these security plan requirements. Our objectives were to assess (1) the progress made to develop, review, and approve facility and

[2]The portwide security plan, called an Area Maritime Security Plan, is to be developed by the Coast Guard's local Captains of the Port and a committee comprised of federal, state, and local agencies; law enforcement and security agencies; and other port stakeholders such as owners and operators of facilities and vessels, trade and labor organizations, and railroad and trucking companies among others. The plan is designed to provide a framework for communication and coordination among port stakeholders and law enforcement officials. Our review focused on plans being developed by entities other than the Coast Guard, and we, therefore, do not discuss these area plans in this report. We will, however, be addressing aspects of these plans in a subsequent report.

[3]See generally 33 C.F.R. Parts 101, 104, and 105. Motorboats and other pleasure craft, for example, are generally, not subject to security plan requirements, as are a variety of other types of vessels below certain prescribed lengths or weights.

[4]This is the present value of costs incurred from 2003 to 2012. Unless otherwise noted, all cost figures cited are present values.

vessel security plans by July 1, 2004; (2) the Coast Guard's monitoring and oversight strategy for ensuring that facility and vessel security plans are implemented; and (3) the accuracy of the Coast Guard's estimates of costs for complying with MTSA security planning and implementation requirements.

To address the first two objectives, we analyzed Coast Guard documents and spoke with officials at Coast Guard headquarters with responsibilities for the security planning process. We also visited seven port areas around the country, choosing locations that reflected diversity in strategic importance, geographic location, and local characteristics.[5] During our visits, we spoke with Coast Guard Captains of the Port;[6] numerous local stakeholders in the private sector; and government officials at the local, state, and federal levels, to understand what progress had been made to develop and implement security plans. We visited Coast Guard officials and contractor staff responsible for reviewing and approving MTSA-required security plans and examined the review and approval process used by the Coast Guard to determine what internal controls were in place to monitor the consistency of the process and ensure compliance with pertinent MTSA requirements. Our work did not include reviewing ports outside the United States or any "foreign-flagged" vessels—vessels registered in countries other than the United States. To address the third objective, we interviewed Coast Guard staff in charge of creating estimates of compliance costs and performed economic simulations to examine the impact of changing the assumptions the Coast Guard used in making its estimates. We asked Coast Guard officials responsible for these cost estimates what steps they took to ensure the reliability of the underlying data on which the estimates were based. We also reviewed the public comments provided to the Coast Guard on its estimates. Our work, which was conducted from June 2003 through June 2004, was done in accordance with generally accepted government auditing standards.

[5]Appendix I describes our scope and methodology in more detail and contains a list of ports we visited and port stakeholders we interviewed.

[6]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 port in which assigned. Captains of the Port enforce, within their respective areas, port safety and security and marine environmental protection regulations. There are 45 Captains of the Port nationwide.

Results in Brief

Although owners and operators have made progress in developing security plans, the extent to which the Coast Guard will have reviewed and approved the approximately 12,300 individual facility or vessel plans by July 1, 2004, varies considerably. Owners and operators are developing about 5,900 plans under an option allowing them to self-certify that the plans will be developed and implemented by July 1. In doing so, they are using standards and templates their trade association had developed and the Coast Guard had approved. Owners and operators who chose this option did not have to submit their plans for review and approval. The Coast Guard's first look at many of these plans will likely not come until after July 1, when inspectors begin compliance inspections to ensure that plans have been implemented. The remaining 6,400 plans, which were not developed through the self-certification process, underwent a detailed review process for which the Coast Guard hired contractors with security experience. The contractors conducting much of the review found that all of these plans needed to be revised, some extensively, and the Coast Guard concurred with the contractors' findings. As of June 2004—1 month before the deadline—-more than half of these plans were still in process. To speed up the process, the Coast Guard added more personnel and began working more directly with owners and operators. Nonetheless, many of these plans will not be approved by July 1. Under MTSA and Coast Guard regulations, facilities and vessels without approved plans would have to cease operations. However, MTSA and the regulations also allow the Coast Guard to grant permission to such facilities and vessels to continue operating for up to 1 year after the plans are submitted on the condition that they continue to make sufficient progress through the review process toward the approval of their plans. The Coast Guard is currently allowing such facilities and vessels to operate through October 31, 2004.

In late May 2004, the Coast Guard issued its strategy for ensuring that facility and vessel owners and operators implement the security activities identified in their plans. It is clear that this strategy will face several challenges, both in the short and longer term. One challenge is the sheer size of the immediate effort: between July and December 2004, the Coast Guard plans to conduct on-site inspections of every facility and as many vessels as possible to ensure that owners and operators are complying with the actions called for in their security plans. Inspectors will have to make decisions about whether owners and operators have identified all vulnerabilities and adequately addressed them. These decisions are complicated, in part because owners and operators have considerable choice in how to mitigate vulnerabilities and because the Coast Guard will be seeing many of these plans for the first time. Other challenges include

ensuring that enough inspectors are available, training them adequately, and equipping them with useful guidance for making on-site inspection decisions. In the short term, these challenges are formidable, because the Coast Guard expects to handle the added July-December inspection load mainly by using reservists with widely varying degrees of training and experience. In the longer term, when the Coast Guard plans to conduct annual compliance inspections for the approximately 12,300 facilities and vessels, it faces the challenge of ensuring that owners and operators continue implementing their plans. In this regard, our work has shown that there are options the Coast Guard could consider beyond regularly scheduled visits, such as unscheduled, unannounced visits and covert testing to help ensure owners and operators do not mask security problems in ways that do not represent the normal course of business.

The accuracy of the Coast Guard's $7.3 billion estimate of maritime industry costs for developing and implementing their security plans is uncertain. An estimate's accuracy is often tied to such factors as the complexity or straightforwardness of the issue, the quality of data and validity of assumptions, and the length of time available to conduct the work. The Coast Guard was heavily limited in all these factors. First, the issue was complex: for example, facilities and vessels are very diverse and they vary greatly in the degree to which they already have security measures in place. Second, to account for such differences, the Coast Guard was faced with having to develop many assumptions, and while the Coast Guard used government and industry expertise to help make these assumptions, it had limited data with which to work, and the potential margin for error was considerable. Our analysis found that changes in the Coast Guard's assumptions could raise or lower the estimate by more than $1 billion. Third, the Coast Guard had only a few months to develop the estimate. The Coast Guard vetted the estimate with stakeholders as a way of testing its reliability, but stakeholders were basically in no better position than the Coast Guard to generalize from their own specific situations. The Coast Guard appeared to make a good-faith effort to prepare an estimate and seek review of it from port stakeholders, but the limiting factors discussed here indicate the result can be viewed more as a rough indicator of costs, not a precise measure.

We recommend that the Coast Guard evaluate the compliance inspection efforts it takes during the initial 6-month period after July 1 and use the results as a means to strengthen its long-term strategy for ensuring compliance. As part of this strategy, the Coast Guard should clearly define inspector qualifications, link these qualifications to a certification process, and consider including unscheduled and unannounced inspections and

covert testing. The Coast Guard reviewed our report and generally agreed with the facts and recommendation.

Background

MTSA mandated major changes in the nation's approach to maritime security. The act called for a comprehensive security framework—one that included planning, personnel security, and careful monitoring of vessels and cargo. Among its specific provisions were the development of systems for tracking vessels, identifying maritime workers, and assessing foreign ports for security risks they posed for the United States. One of MTSA's central components is a systematic approach to strengthening security throughout the nation's port areas—a difficult task, given the tremendous size and variety of activities and user groups involved. Ports present attractive targets: they are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks designed to move cargo and commerce as quickly as possible. They contain not only terminals where goods bound for import or export are unloaded or loaded onto vessels, but also other facilities critical to the nation's economy, such as refineries, factories, and power plants.

Facilities and vessels can be vulnerable on many security-related fronts. Facilities such as container terminals, where containers are transferred between ships and railroad cars or trucks, must be able to screen vehicles entering the facility and routinely check cargo for evidence of tampering. Chemical factories and other installations where hazardous materials are present must be able to control access to areas containing dangerous goods or hazardous substances. Vessels, ranging from oil tankers and freighters to tugboats and passenger ferries, must be able to restrict access to areas on board the vessel such as the bridge or other control stations critical to the vessel's operation. To reduce the opportunity for terrorists to exploit these vulnerabilities, as well as to help minimize the effects of accidents or natural disasters, facilities and vessels need to take mitigation steps. For example, fences, security guards, and monitoring cameras can all be used to reduce the potential for unauthorized entry and help prevent vulnerabilities from being exploited.

Dealing with such vulnerabilities involves a careful balance between the benefits of added security and the potential economic impacts of security enhancements. While there is broad support for greater security, this task is a difficult one because the nation relies heavily on a free and expeditious flow of goods. Particularly with "just in time" deliveries, which require a smooth and expeditious flow through the transportation system,

delays or disruptions in the supply chain could have serious economic impacts. Striking the right balance between increasing security and protecting economic vitality of the national economy and individual port stakeholders will remain an important and difficult task. It is also important to keep in mind that total security cannot be bought no matter how much is spent on it. It is difficult if not impossible to successfully anticipate and thwart all types of potential terrorist threats that highly motivated, well skilled, and adequately funded terrorist groups could devise.

In this environment, MTSA required owners and operators of facilities and vessels to conduct assessments that would identify their security vulnerabilities and to develop security plans to mitigate these vulnerabilities. Under the Coast Guard's implementing 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. [7] The plans are "performance-based," meaning that the security outcomes were specified, but the stakeholders were free to identify and implement whatever measures they desired as long as these measures achieved the specified outcomes. MTSA tasked the Secretary of the Department of Homeland Security with responsibility for reviewing, approving, and overseeing the implementation of these plans, and the Secretary delegated this task to the Coast Guard.

MTSA imposed a specific date, July 1, 2004, for facilities and vessels to begin operating in compliance with the plans. The Coast Guard decided to adopt a schedule that would align the United States with ongoing international improvements in maritime security as well as the act. In December 2002, members of the International Maritime Organization (IMO) adopted the International Ship and Port Facility Security (ISPS) Code, an international agreement that called for security plans to be in

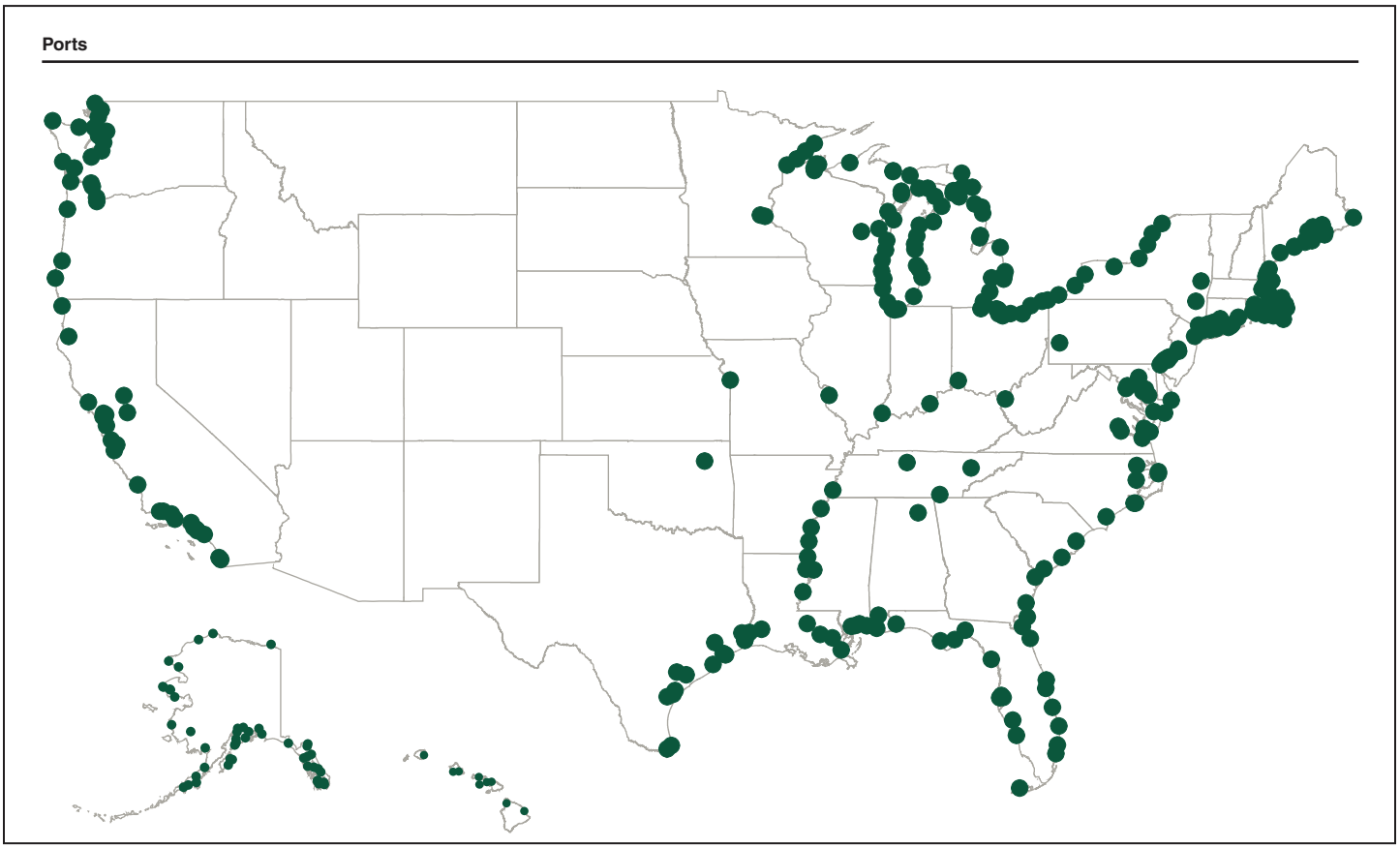
[7]The requirements for security plans are found in 33 C.F.R. Part 104, Subpart D for vessels and 33 C.F.R. Part 105, Subpart D for facilities. See appendix II for a listing of required security plan contents.

place by July 1, 2004.[8] The Coast Guard had to decide which facilities and vessels were subject to MTSA's requirements and develop an approach for reviewing and approving the plans. The categories of facilities and vessels were specified in implementing regulations, issued in final form on October 22, 2003.[9] Overall, approximately 3,150 facilities and 9,200 vessels operating in more than 300 ports around the nation were required to comply with these requirements. The ports included not only those on the Atlantic, Gulf, and Pacific coasts, but also ports in the Great Lakes and various inland waterways like the Mississippi and Ohio rivers. (See fig. 1.)

[8]IMO is responsible for improving maritime safety, including combating acts of violence or crime at sea. The United States is a member. In November 2001, the Commandant of the Coast Guard addressed IMO's General Assembly, urging that body to consider an international scheme for port and shipping security. Recommendations and proposals for comprehensive security requirements, including amendments to International Convention for Safety of Life at Sea, 1974, (SOLAS) and the new ISPS Code, were developed at a series of intersessional maritime security work group meetings held at the direction of IMO's Maritime Safety Committee.

[9] Prior to issuing the final regulation, the Coast Guard issued an interim final rule on July 1, 2003.

Figure 1: Location of U.S. Ports



Source: GAO presentation of Bureau of Transportation statistics, TSA, and FTA data.

The key dates in the process established by the Coast Guard included the following:

- By December 31, 2003, those facilities and vessels subject to MTSA's security plan requirements had to submit security plans to the Coast Guard for review or self-certify that their plans would be developed and implemented by July 1.

- By July 1, 2004, the Coast Guard intends to complete its review and approval of the security plan materials from all facilities and vessels. On that date, facilities and vessels are to have their security plans implemented.

- By January 1, 2005, the Coast Guard intends to conduct on-site inspections of each facility subject to the security plan requirements, along with as many vessels as possible, to ensure that the steps called for in the security plan are actually in place.[10]

- By July 1, 2005, the Coast Guard intends to complete the remaining on-site compliance inspections for vessels it is not able to inspect by January 1, 2005.

The Coast Guard took a number of steps to help stakeholders understand and comply with requirements. The Coast Guard issued updated guidance and established a "help desk" to provide stakeholders with a single point of contact, both through the Internet and over the telephone. At the local level, Coast Guard marine safety offices[11] at the ports provided stakeholders operating within their ports additional information and assistance through forums, training sessions, e-mails, letters, and telephone calls. The Coast Guard also hired two contractors[12] to provide expertise in reviewing the facility and vessel security plans.

In issuing the final rules, the Coast Guard also developed an estimate of the cost to implement MTSA's port security provisions. The Coast Guard estimated that implementing the various port and vessel security provisions, including the security plans, would cost $7.3 billion over 10

[10]The Coast Guard also intends to complete on-site inspections of "uninspected vessels" by December 31, 2004. These "uninspected vessels" include some towing vessels, most fishing industry vessels, some freight barges, and certain passenger vessels, among others that were not required to submit a security plan but did so voluntarily.

[11]Marine safety offices are located at coastal ports and on inland waterways and are responsible for the overall safety and security of maritime activities and for environmental protection in their geographic areas.

[12]The Coast Guard hired Black and Veatch Corporation, an engineering consulting and construction company with expertise in facility security, to conduct the facility security plan reviews. The Coast Guard also hired George G. Sharp, Inc., a maritime engineering, safety, and security company with expertise in vessel security, to conduct the vessel security plan reviews. The Coast Guard is reviewing the security plans with the contractors in two locations: The National Facility Security Plan Review Center in Overland Park, Kansas, and the Marine Safety Center (for vessels) in Washington, D.C.

years.[13] In fiscal years 2002-2004, the federal government awarded $516 million in grant funds for improvements in port security; in fiscal year 2005, the Department of Homeland Security expects another $50 million to be made available through federal grants to implement security improvements identified in the plans. However, the bulk of the cost burden is likely to be borne by facility and vessel owners and operators.

Extent of Coast Guard Review and Approval of Individual Plans Varies Widely

While the Coast Guard expects owners and operators to implement the approximately 12,300 facility and vessel plans by July 1, 2004, the extent it will have reviewed and approved these plans varies widely, for two main reasons. First, about 5,900 of these plans were developed under an option that essentially deferred Coast Guard review of individual plans until after July 1. Under this option, owners and operators self-certified that their plans would be based on industry-developed, Coast Guard-approved standards and templates. Owners and operators choosing this option did not have to submit their plans for review. Second, while the remaining 6,400 plans did undergo detailed review, all of them had deficiencies, and many are not likely to be corrected and fully approved by July 1. Under MTSA and Coast Guard regulations, facilities and vessels without fully approved plans would have to cease operations on July 1. However, the Coast Guard has put procedures in place to allow such facilities and vessels to continue operating after the deadline, provided certain conditions are met.

Two Options for Developing Security Plans Varied in Key Respects

The Coast Guard established two options, referred to in this report as options A and B, which owners and operators could follow in developing their plans. (See fig. 2.) These options differed in the documents that had to be supplied to the Coast Guard and the extent of review that would be applied to individual plans by July 1.

- Option A: Owners or operators who chose this option had to develop their own security plans according to the requirements in the final rules and

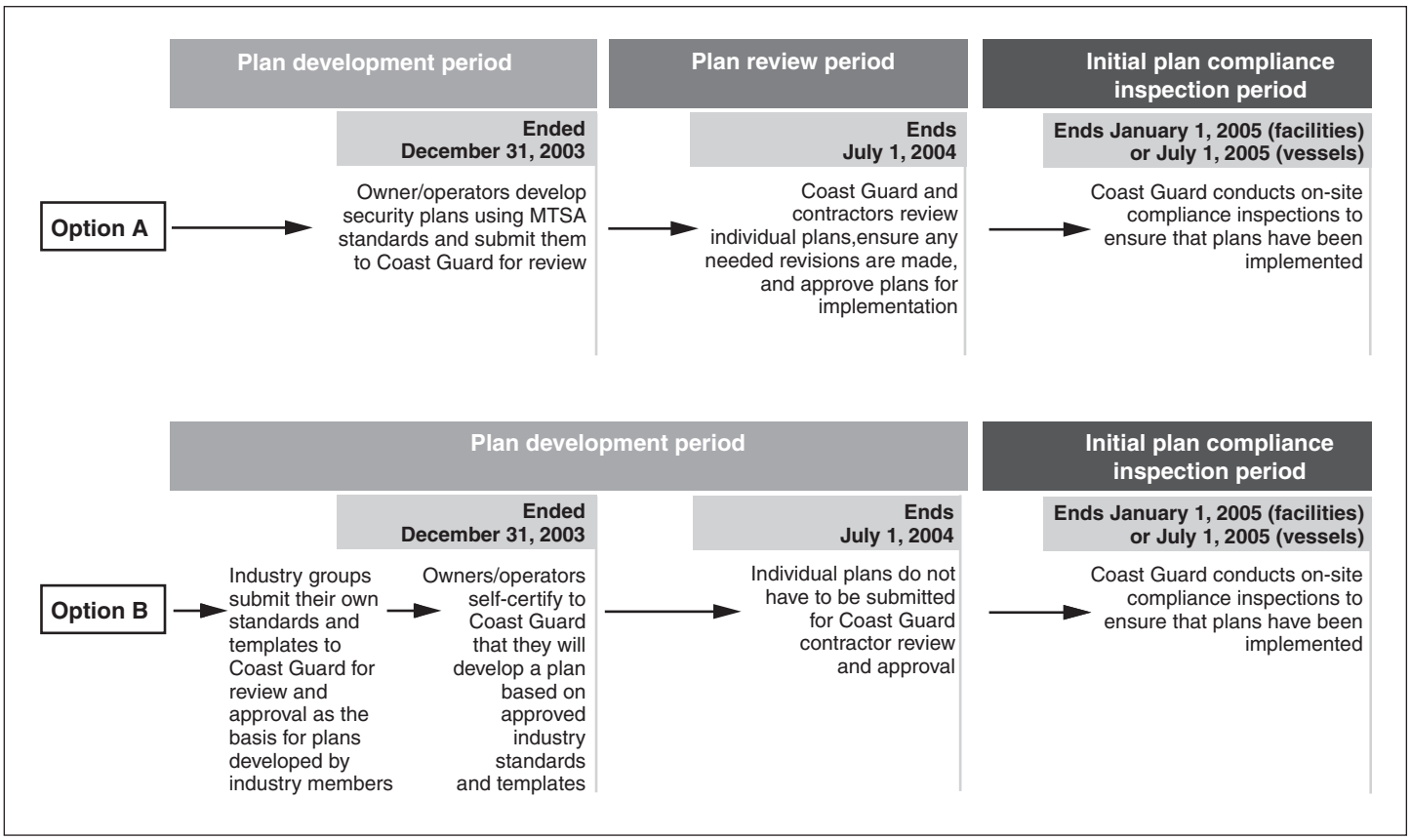
[13]The estimate of $7.3 billion applies to compliance costs at Maritime Security Condition System (MARSEC) Level 1. MARSEC is a three-tiered system developed by the Coast Guard to communicate the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure. The levels align closely with DHS's color-coded Homeland Security Alert System in the following way: MARSEC Level 1 applies when threat conditions Green, Blue, or Yellow are set; MARSEC Level 2 applies when threat condition Orange is set; and MARSEC Level 3 applies when threat condition Red is set.

submit them to the Coast Guard for review by December 31, 2003. These plans were then subject to detailed review by the Coast Guard and its contractors.

- Option B: Owners or operators who were members of certain industry groups could choose this option to develop plans by using Coast Guard approved security programs established by their industry groups, such as an association of chemical manufacturers or passenger vessel operators. To accommodate widespread interest from owners and operators in being able to use such standards to meet MTSA requirements, the Coast Guard allowed trade organizations to submit security standards, including templates[14] for developing security plans, for consideration as "alternative security programs" (ASP). The Coast Guard then reviewed each organization's application and approved those it determined would provide an equivalent level of security to the standards being applied under option A at all threat levels within the nation's Maritime Security Condition System. Members of the industry or trade association then self-certified to the Coast Guard that they were using the standards and templates to develop security plans for their facilities or vessels.

[14] A template is a document that owners or operators can use to develop and implement security plans by tailoring it to the specific circumstances of their operation.

Figure 2: Overview of the Two Options for Developing Security Plans



Source: GAO presentation of Coast Guard data.

These two options both involved review by the Coast Guard, but there was considerable difference in what was being reviewed before the start of the compliance phase on July 1, 2004. Under option A, the Coast Guard and its contractors would review the individual plans themselves; under option B, Coast Guard review would center on the organization's standards and templates and would not extend to the individual plans.[15] These reviews

[15]Under both options, facilities also had to submit a "Vulnerability and Security Measures Summary" (Form CG-6025), which lists the vulnerabilities and specific security measures to be taken. Owners and operators submitting plans under option A also had to submit a security assessment report, a document based on background information and an on-scene survey, identifying possible threats, vulnerabilities, consequences, and existing protective measures. Those who chose option B did not have to submit this report.

were not the same, in that industry standards and templates are a framework for developing a plan, but are not analogous to individual vessel or facility security plans. To adapt the standards and templates to specific facilities and vessels, owners and operators still need to do considerable work.

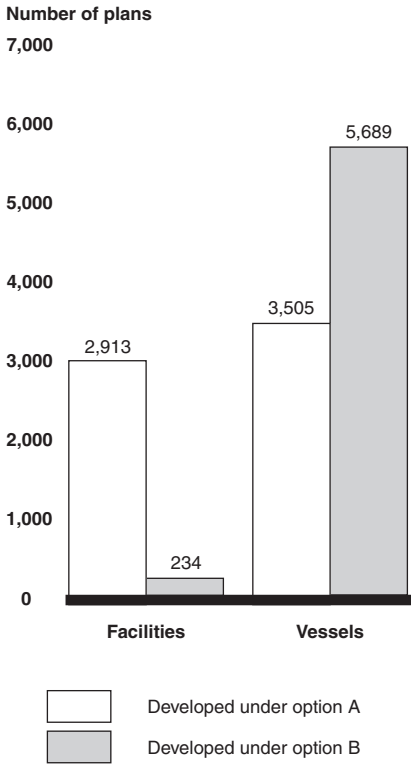
Coast Guard records indicate that 90 percent of facilities and vessels met the December 31, 2003, deadline for complying with one of the two options. Most owners and operators who did not meet the December 31 deadline subsequently complied. However, the Coast Guard issued notices of violation with a $10,000 penalty assessment against owners or operators of 67 facilities and 90 vessels who had not responded by February 1. Eight of these owners or operators received a subsequent $25,000 penalty assessment for not responding by March 1.

Nearly Half of All Plans Will Be Developed under the Option with No Review of Individual Plans

In all, plans for 5,923 facilities or vessels are being prepared under option B. Of these, 234 were facilities and 5,689 were vessels. The Coast Guard granted approval to standards and templates submitted by nine trade organizations, most of them vessel-related,[16] and the plans being developed under this option reflect the larger number of vessel-related groups. Overall, about 7 percent of facility plans are being developed under this option, compared with 62 percent of all vessel plans. (See fig. 3.)

[16] Trade or industry organizations with approved "alternative security programs" include: American Chemistry Council, American Gaming Association, American Waterways Operators, Lake Carriers' Association, Offshore Marine Service Association, and the Passenger Vessel Association. Other organizations that received interim approval: the North American Grain Export Association & National Grain and Feed Association, Greater New Orleans Barge Fleeting Association, and Washington State Ferries.

Figure 3: Distribution of Individual Security Plans by Development Option



Source: GAO analysis of Coast Guard data.

The extensive use of option B meant that nearly half of the individual plans were not directly reviewed by the Coast Guard before they were to be implemented on July 1, 2004. Users of option B had to send the Coast Guard a letter stating which alternative security program they planned to use. The Coast Guard was to check to ensure that the owners or operators were members of the organization that developed the program. Inasmuch as option B reduced the number of individual plans to be reviewed, it lessened the Coast Guard's review workload. However, option B also had the effect of deferring review of these individual plans into the next phase of the process—the on-site compliance inspections to be conducted starting July 1. For these facilities and vessels, the Coast Guard's first look

at the plans will occur when inspectors arrive to ensure that the plans have been implemented.[17]

All Plans Undergoing Individual Review Had Deficiencies that Affected Final Approval

For plans submitted under option A, the Coast Guard established a comprehensive review and approval process that relies on contractors with security planning expertise to review and evaluate the plans. Plans move through a two- or three-stage process, depending on whether they are for vessels or facilities. In stage I, at least two contract personnel independently reviewed the plans to ensure they contain material covering all required items such as measures for access control, responses to security threats, and drills and exercises to train staff and test the plan. Plans passing this stage move to stage II, where comprehensive assessments are conducted as to whether the plans address all of MTSA's requirements. Vessel plans are approved once the Coast Guard determines they have passed this stage II review. Facility plans continue on to a stage III review, in which the local Coast Guard marine safety office verifies the information in the security assessment against the facility's physical characteristics and determines whether the plan is adequate to meet security needs. This last stage may include an on-site visit, but if conducted, this verification review is not the same as the post-July 1 compliance inspection for determining whether the facility has implemented the plan. Facility plans are approved once the Coast Guard determines they have passed this stage III review.

This review and approval process flagged problems. Every one of the more than 6,400 facility and vessel plans submitted under this option had deficiencies that needed to be revised before the plan could be approved. As table 1 shows, of the 2,913 facility plans and 3,505 vessel plans submitted under option A, more than half were still undergoing the detailed review as of June 2004. Most of these plans still in review were facility security plans.

[17]The Coast Guard has issued guidance to Captains of the Port to encourage them to "engage" with users of option B to review their progress prior to July 1, 2004. However, these users are not required to agree to these reviews.

Table 1: Progress of Facility and Vessel Security Plan Review Under Option A as of June 2004

	Stage I	Stage II	Stage III	Approved	Totals
Facility security plans	80	1,637	1,076	120	**2,913**
Vessel security plans	23	750	[a]	2,732	**3,505**

Source: GAO presentation of Coast Guard data.

Note: Facility security plan numbers are as of June 14, 2004; vessel security plan numbers are as of June 4, 2004.

[a]Vessel security plans are approved once the Coast Guard determines they have passed stage II.

The problems identified through this process resulted from a variety of deficiencies in the plans developed under option A. The most common deficiency identified for both facility and vessel plans during stage I, according to the Coast Guard, was the failure to address or inadequately address all of the required security plan sections specified in regulations. For example, some owners and operators simply restated the text in the regulations or excluded some plan elements such as the security assessment. Common stage II deficiencies for facility plans included providing insufficient detail describing steps to be taken for elevated MARSEC threat levels or security measures to be put in place for control of access to the facility. For vessel security plans, common deficiencies identified at this level were inadequate descriptions of the steps for conducting security drills and exercises, insufficient measures for controlling access, or inadequate descriptions of the qualifications and responsibilities of those in charge of security programs.

Resolving such deficiencies has kept many plans at stage II of the review. After reviewing the contactor's findings, the Coast Guard notified the owner or operator about the deficiencies and any deadline for submitting revisions.[18] While owners and operators could correct some deficiencies easily, such as adding a missing telephone number or name of a security officer, other corrections required more work, such as providing more detail about access control procedures or measures. Plans could not proceed to the next stage until the Coast Guard was satisfied they were complete—a process that has sometimes required repeated revision.

[18] For revisions to facility security plans, 30 calendar days were allowed for revisions to be made and resubmitted to the Coast Guard. No time limit was specified for revisions to vessel security plans.

Correcting these deficiencies has taken longer than the Coast Guard anticipated.[19]

Process Exists to Allow Facilities and Vessels with Unapproved Plans to Continue Operating

Under MTSA and Coast Guard regulations, facilities and vessels can be shut down if they have not complied with the requirements called for under options A or B by July 1, 2004. Facilities and vessels with plans still in revision under option A could thus face closure. To speed up the overall process, the Coast Guard adopted a strategy called "compliance through engagement." Instead of sending deficiency letters, the Coast Guard began calling owners and operators directly to review deficiencies, explain regulatory requirements, and answer questions. The Coast Guard also advised Captains of the Port to encourage facility owners or operators still in stage I to make needed revisions so the plan could pass to stage II. Staffing was also increased at the center reviewing facility security plans to help speed review.[20] According to the Coast Guard, this strategy significantly improved turnaround time for receiving revised plans from owners and operators.

Anticipating that plans for some facilities and vessels would still be in process on July 1, the Coast Guard also took steps to allow most of them to continue operating as allowed by MTSA and the regulations.[21] The steps vary depending on whether the plan covers a facility or vessel and how far along it is in the process.

- Facilities that have received an initial stage II review can receive interim approval of their plan through October 31, 2004, pending final approval of the security plan. Rather than waiting to conduct on-site verification reviews until plans move to stage III, the Coast Guard advised Captains of the Port to have their inspectors begin visiting all facilities that had received a stage II review, regardless of whether the facility had revised

[19]Some owners or operators with plans undergoing the review process have commented that the Coast Guard's contractors have been unnecessarily "nitpicky" or have gone beyond regulations, resulting in what the owners or operators consider to be excessive deficiencies. While we did not evaluate the validity of these comments, Coast Guard officials have publicly defended the quality of the contractors' performance.

[20]The Coast Guard is reviewing the facility security plans with the contractor at the National Facility Security Plan Review Center in Overland Park, Kansas.

[21]MTSA allows the Coast Guard, under certain circumstances, to grant permission to facilities and vessels with plans still in process to continue operating for up to 1 year after the plans were submitted.

the deficiencies identified through the review. During these visits, Coast Guard personnel are to verify that (1) the plan accurately reflects the facility and its operations, (2) the proposed security measures are realistic, and (3) deficiencies will either be addressed by July 1 or satisfactory interim measures will be in place. If these conditions are met and the changes to the plan are administrative in nature, the Coast Guard may issue interim approval allowing continued operations.

- Vessels that have received an initial stage II review can receive similar interim approval of their plans through October 31, 2004. The Coast Guard Marine Safety Center reviewing vessel plans can issue such approvals provided they are satisfied that the plans are sufficiently complete and any needed changes are administrative in nature.[22]

- Facilities and vessels that are not far enough along to receive interim approval of their plans—for example, still making substantial revisions to their plans—can also receive permission to continue operations. The process is much the same as that described earlier for interim approval. For facilities, after an on-site visit the Captain of the Port may issue a letter to the owner or operator, identifying the areas of the plan requiring significant revision and allowing the facility to continue operations through October 31, on the condition that temporary security measures are implemented while the security plan continues to be reviewed. For vessels, the Marine Safety Center reviewing the plans may similarly issue a letter authorizing a vessel to continue operating, as long as conditions specified in the letter are met while review of the plan continues.

- These approaches do not extend to facilities or vessels that have not completed stage I of the review process. The Coast Guard will not allow those facilities and vessels to operate after June 30, 2004. Thus, owners or operators who have not submitted a complete facility plan for Coast Guard review are to be shut down. According to the Coast Guard, MTSA provides the Coast Guard with the necessary legal authority to shut down any facilities or vessels in this situation, if necessary.[23]

[22]Vessels in international trade were given priority since all vessels subject to the SOLAS/ISPS codes must be in compliance with an approved security plan by July 1, 2004.

[23]In addition, the Captain of the Port has the authority under 33 C.F.R. Part 6 to establish security zones and prevent access to any vessel or facility whenever he or she believes such action may be necessary to prevent damage or injury.

Strategy for Monitoring and Oversight of Plan Implementation Faces Numerous Challenges

In late May 2004, the Coast Guard issued its strategy for monitoring and overseeing the implementation of security plans after July 1.[24] It is clear that this strategy faces a number of challenges both in the short and longer term. The first challenge is the amount of work required to conduct the initial review of compliance inspections. Between July and December, the Coast Guard plans to inspect every one of the 3,147 facilities and as many of the 9,194 vessels as possible to ensure that owners and operators are complying with the actions called for in their security plans.[25] These inspections will need to determine whether vessel and facility operators have identified all vulnerabilities and adequately addressed them—a task made more difficult by the fact that most of the 5,923 plans developed under option B will not have received detailed review. Other challenges facing the Coast Guard include ensuring that enough inspectors are available, training them appropriately, and equipping them with sufficient guidance to make difficult judgments about whether owners and operators have taken adequate steps to address vulnerabilities. The Coast Guard's attention has been understandably focused on how to meet these challenges in the immediate "surge" of monitoring activity between July and December.[26] However, in the longer term, when the Coast Guard plans to conduct annual compliance inspections for the more than 12,300 facilities and vessels, it faces the challenge of developing a strategy to ensure that owners and operators continue implementing their plans.

[24]The guidelines for this strategy were contained in *Navigation and Vessel Inspection Circulars* (NVIC), 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.

[25]The Coast Guard plans to complete all vessel inspections by July 1, 2005, and as soon after July 1, 2004, as possible. Each vessel will receive a security compliance inspection concurrently with its annual Certificate of Inspection visit conducted by the Coast Guard between July 1, 2004, and July 1, 2005. However, under three situations vessels will receive inspections earlier. First, all inspections for SOLAS vessels (i.e., U.S. registered vessels operating internationally) must be completed by July 1, 2004. Second, at the discretion of the Captain of the Port, certain vessels of interest will be inspected shortly after July 1, 2004. Finally, the Coast Guard will inspect any vessel whose owners or operators request an early security compliance inspection.

[26]The Coast Guard refers to this initial 6-month period as a surge effort because of the amount of work demanded in a short time frame. The Coast Guard regards the facility compliance inspections, which must be completed in full within this period, as particularly time-consuming.

Workload for Compliance Inspections Is Substantial, Potential Exists for Finding More Vulnerabilities, and Assessing the Adequacy of Security Preparation Is Difficult

The initial volume of compliance inspections to be done is large and time is limited. The Coast Guard expects to complete the first round of on-site inspections of all 3,147 facilities, as well as the inspection of as many vessels as possible, by January 1, 2005. During these compliance inspections, inspectors are to assess the steps that each port stakeholder has taken to put a security plan into place, such as the extent to which access controls like fences, guards, gates, and cameras are in place, or the extent to which the security drills written in the plan are actually being conducted.[27] Since most of the 5,923 plans developed under option B were not reviewed by the Coast Guard or its contractors, inspectors will also have to consider not only whether these plans have been implemented but also whether they adequately identify relevant vulnerabilities and specify sufficient steps to address them.

One reason for caution with regard to the adequacy of option B plans is that there are indications that some owners and operators using option B may not be fully aware of what they have to do to develop sufficient plans, or, if they are aware of it, may be slow in complying. For example:

- According to the Coast Guard's MTSA security plan program manager, the agency's interactions with option B users showed that some of them erroneously believed that membership in an industry or trade organization with approved standards and templates satisfied their obligation to implement a security plan.

- In some cases, the use of option B appeared to be a way of postponing the completion of a security plan. For example, after being advised by the Coast Guard that he missed the deadline for submitting a security plan, one stakeholder joined an industry organization for the sole purpose of using option B to avoid having to immediately write a security plan. Another vessel operator we visited 2 weeks before the deadline to submit security plans said he was using option B as a means to gain an extra 6 months to complete the security plan.

Even among plans developed and reviewed under option A, there are indications that the inspections may reveal additional vulnerabilities or,

[27]A drill is a training event that tests at least one component of the vessel or facility security plan and is used to maintain a high-level of security readiness. According to the Coast Guard regulations, at least one security drill is to be conducted by owners and operators every 3 months.

for cost reasons, the disparity between actions prescribed in the plans and actions actually implemented. For example:

- An official at a major port told us that more security vulnerabilities were known than were included in the facility security plan, these vulnerabilities were not included because money was not available to address them. This port official said the port would await the Coast Guard's review to see if the Coast Guard would identify any of these vulnerabilities and require mitigating actions.

- Several owners and operators of facilities and vessels also told us that funding was a major challenge. Although they did not indicate that they omitted vulnerabilities from their plans, these owners and operators told us that it would be difficult to obtain the financial resources to fully mitigate their known vulnerabilities.

Compliance inspections will also be challenging because they involve subjective evaluations about the adequacy of security measures. The facility and vessel plans created by port stakeholders are performance-based, meaning the Coast Guard has specified the outcomes it is seeking to achieve and has given port stakeholders responsibility for identifying and delivering the measures needed to achieve these outcomes. While this approach provides flexibility to owners and operators in designing and implementing their plans, it also places a premium on the skills and experience of inspectors to identify deficiencies and recommend corrective action. For example, inspectors will have to determine if the security measures outlined in the approved security plan adequately address the security vulnerabilities identified in the security assessment, which the Coast Guard regards as by far the most difficult step in the compliance inspection process.

Whether Sufficient Inspection Personnel Will Be Available Is Not Clear

Another challenge the Coast Guard faces is ensuring that it has enough qualified inspectors to complete all the inspections required during the surge period. The Coast Guard estimated the need for and then allocated an additional 282 positions, or "billets," to local marine safety offices to supplement existing inspectors during this period. The Coast Guard did not have a great deal of workload data to use in making this estimate; as we have pointed out in other reports, the agency does not have a system in place for determining how much time its personnel are spending on

specific duties.[28] The Coast Guard told us that it made its determination of how many additional positions would be needed by using working groups, expert panels, available data, and information about resources in port security missions since the September 11, 2001, terrorist attacks.[29] While the Coast Guard thus had some basis for determining how many more staff it should assign to complete the work on time, the approach stops well short of providing demonstrable evidence of its validity. The Coast Guard based its projection in part on past experiences with environmental and safety inspections, but whether those types of inspections are analogous is unclear. Further, the Coast Guard could not provide documentation of the approach it used, limiting its ability to assess the adequacy of its decision.

The Coast Guard also faces challenges in ensuring that it has the right mix of skills and experience among these additional personnel. The Coast Guard's staffing estimate does not specify what rank or type of personnel are required to complete the surge inspections. According to Coast Guard documents, none of the job functions for the additional 282 personnel working on compliance inspections have been detailed. Further, of the additional 282 positions, about 75 percent are reservists who are scheduled to be available for only a limited time. Most are scheduled for deactivation in October 2004 – in the middle of the surge period – though the Coast Guard has the ability to extend their tour of duty. All of these challenges – the uncertainty of the estimate, the lack of specificity about what personnel are needed, and the reliance on personnel who may become unavailable — increase the overall challenge of ensuring that the first round of compliance inspections is effective, especially given the subjective evaluations that are required.

Training Will Need to Overcome Disparity in Skills and Experience among Inspectors

The skills and prior inspection experience of the reservists who will be assigned to supplement existing inspectors varies widely. Some have graduate degrees in security management, while others have no formal security training or prior experience. For example, in New Orleans, 1 of 7 reservists assigned to support local inspectors had previous inspection experience, while in New York, at least 9 out of 19 reservists assigned to

[28]U.S. General Accounting Office, *Coast Guard: Relationship Between Resources Used and Results Achieved Needs to Be Clearer*, GAO-04-432 (Washington, D.C.: March 22, 2004).

[29]The working groups were comprised of Coast Guard headquarters, area, district, and field office staff. The historical information came from the Coast Guard's implementation of the Oil Pollution Act of 1990, Public Law 101-380, 104 Stat. 484 (1990).

this task had previous inspection experience. The disparity in experience levels raises the possibility that personnel with little inspection experience will be less able or equipped to identify deficiencies or assess the adequacy of security efforts. This has implications for creating variation in the rigorousness with which inspections are conducted from location to location and port to port.

The Coast Guard has acknowledged this disparity and is taking steps to address it, but these steps still carry challenges:

- The Coast Guard developed required training for all staff who would be conducting port security compliance inspections. This training lasted for 5 days and consisted of computer-based instruction, classroom training from security experts, and other coursework.[30] It could be completed either by attending program sessions at various locations or through tutoring from other staff who had attended the training. As of mid-June, the Coast Guard reported that more than 500 persons had completed this training. Whether this training will be sufficient to overcome the skill and experience disparities among inspection staff remains uncertain, particularly since some inexperienced staff may receive the training second-hand. Coast Guard officials said that one reservist with little experience might be sent to the training, while another with similar experience might be taught by a fellow reservist who attended. Thus, a challenge the Coast Guard faces is to discern the extent to which each inspector has mastery of the subject matter.

- To emphasize on-the-job-training and to try to improve the consistency during the compliance inspection process, the Coast Guard plans to pair inspectors with little previous experience with more experienced inspectors. This will be especially critical when reviewing the 234 facilities and 5,689 vessels using option B plans, since those plans did not undergo a detailed review. However, the time that reservists will need for such on-the-job experience before they can contribute to the inspection process is unknown and could affect the quality of the inspections and the Coast Guard's ability to complete all of the inspections during this surge period.

[30]The first 2 days of the 5-day training were not required for those personnel with prior inspection experience because the first 2 days covered "basic" elements of conducting inspections.

Developing Inspection Guidance for a Performance-Based Inspection Process Is Difficult

A concern consistently raised by stakeholders is that if enforcement of the security requirements varies from port to port, there will not be a uniform standard of security across the nation. This inconsistency has two main effects: First, it may create the potential for disparities in stakeholder compliance and gaps in security. Second, aside from the potential implications on security, stakeholders operating in a port where enforcement is more rigorous could be put at a competitive disadvantage, in that they may have to spend more money implementing security measures than required of similar stakeholders in other locations. Stakeholders are concerned that such disparities could affect competitiveness among companies in the same industry or, on a broad level, competition among ports themselves.

The Coast Guard is aware of this issue, and its preparations include ways to make the security inspection process more uniform. In addition to the training program, the Coast Guard issued an inspection guide that all inspectors will use during on-site inspections.[31] The primary tool in the guide is a checklist that inspectors can use as a "roadmap" to ensure that all areas of the security plans are covered when inspecting a facility or vessel. The guide also provides inspectors with scalable recommended penalty measures to consider, given the severity and nature of the deficiencies found during an inspection.

While a compliance guide is likely to provide some assistance to the inspector, a key challenge to its usefulness during this surge inspection period is the performance-based nature of the evaluation, which makes it difficult to cover all the circumstances an inspector may encounter. Inspectors will not check for compliance with a specific procedure; instead, they will have to make a judgment about whether the steps the owner or operator has taken, considered together, provide adequate security. Although the security plans are required to contain similar elements, they do not have to be identical, nor do they need to address security vulnerabilities using the same mitigations. Facilities and vessels may have different – yet reasonable – methods for addressing the same vulnerability. This subjective nature of the evaluation process has raised concerns among port stakeholders. Given their experience with existing Coast Guard safety and environmental inspection programs, several local

[31]The inspection guide, checklists, and other enforcement guidance were included in a series of NVICs issued by the Coast Guard. The NVICs that included the inspection guides were issued in May 2004.

port stakeholders we spoke with said they did not think the Coast Guard had been consistent in its administration of regulations across inspectors and offices. These port stakeholders said they did not think the same standards had been applied to other, similar operations as were applied to their own organization. We did not assess the validity of these concerns, but the Coast Guard regards this issue as the greatest implementation challenge the agency faces.

Lessons Learned during Surge Period Should Help in the Development of Strategy for Longer-Term Monitoring and Oversight Responsibilities

While the Coast Guard is understandably focused on the initial surge period for compliance inspections, it will soon need to decide how to staff and conduct inspections on a longer-term basis. Accordingly, what Coast Guard officials learn during the surge phase should help them determine how to staff and conduct effective compliance inspections. Many of the elements of this longer-term strategy will likely have to deal with the same basic challenges faced during the surge period: ensuring that enough personnel are available, training them well, and equipping them with necessary guidance. These challenges will be particularly important to overcome considering the frequency with which Coast Guard personnel rotate to new positions within the Coast Guard.[32] Port stakeholders told us that the discontinuity caused by these rotations creates gaps in expertise among personnel, which ultimately leads to inconsistent application of the regulations. According to Coast Guard officials, becoming a fully proficient inspector takes time, and when inspectors do become proficient they often face reassignment.

To address MTSA requirements and coordinate with its other annual inspections, the Coast Guard plans to conduct security plan compliance inspections annually for each of the more than 12,300 facilities and vessels. MTSA requires that facility and vessel owners and operators update and resubmit their security plans to the Coast Guard every 5 years or whenever a substantial change is made to their facility or vessel. As another component of its longer-term compliance strategy, the Coast Guard stated in its recently issued guidance that Captains of the Port may verify continued compliance with the security plans at any time through intervening inspections between the required annual inspections. This critical responsibility of providing effective national maritime security

[32]Every 2 to 4 years, the Coast Guard rotates its staff among various duty stations, such as search and rescue, high- and medium-endurance cutters, and buoy tenders. The Coast Guard also rotates its staff within duty stations, such as moving facility security inspectors to noninspection duties within a marine safety office.

through monitoring and oversight emphasizes the importance of a sound longer-term strategy.

While the strategy has yet to be implemented, it is important that challenges be overcome in order to help ensure detection of noncompliance with MTSA requirements. As the Coast Guard continues to enhance its strategy, there are other options it can consider besides regularly scheduled annual compliance inspections and the intervening inspections. For example, our work assessing other areas such as airport security and regulatory compliance[33] has identified approaches for ensuring compliance and improving and strengthening security such as unscheduled and unannounced inspections, on weekends or after normal working hours,[34] and covert testing.[35] In fact, Coast Guard officials responsible for facility and vessel inspections indicated that unscheduled inspections would be a positive component of a longer-term strategy because informing owners or operators of annual inspections can allow them to mask security problems by preparing for inspections in ways that do not represent the normal course of business.

Cost to Comply with MTSA Is Uncertain

Although the Coast Guard made a good-faith effort in preparing its estimate of $7.3 billion for maritime industry compliance with MTSA security-related requirements, the estimate needs to be viewed with some caution, because (1) the Coast Guard had to assume values for a number of cost factors for which there was incomplete data and (2) it had limited time to prepare the estimate. The Coast Guard was unable to gather further information to ensure the accuracy of these values or to determine how other values for these same factors would affect cost.

The $7.3 billion estimate covers a 10-year period of time (2003-2012) and more than 90 percent of it is for the costs to be incurred by vessel and facility owners to increase security. The Coast Guard estimated the cost of

[33]U.S. General Accounting Office, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, GAO-04-728 (Washington, D.C.: June 4, 2004).

[34]Since facilities and vessels are often staffed differently on weekends, evenings, and nights, this approach is intended to allow inspectors a better opportunity to identify the actual operating conditions of facilities and vessels.

[35]Covert testing would involve Coast Guard agents working undercover to evaluate, among other things, the effectiveness of security processes and procedures.

securing facilities at $5.4 billion and the cost of securing vessels at $1.4 billion. (The remaining portion of the estimate was for outer continental shelf facility security, area maritime security, and automatic identification system requirements.) Appendix III explains how the Coast Guard developed these estimates.

The accuracy of an estimate is often tied to such factors as the complexity or straightforwardness of the issue, the quality of data and validity of the underlying assumptions, and the length of time available to do the work. The Coast Guard faced a number of challenges in dealing with each of these factors. Major challenges included the following:

- **Limited opportunity for expert involvement**. Although the Coast Guard worked with a panel of experts to develop the estimate, Coast Guard officials said that time limitations precluded making the panel as widely representative of industry and government as possible. They also said that time limitations precluded an extensive set of meetings over the course of many months, which would have allowed the expert panel to make more useful contributions.

- **Limited opportunity to analyze data or to test the uncertainty of estimates**. The Chief of the Standards Evaluation and Analysis Division, who was the official responsible for developing the estimate, said that if more time had been available, the Coast Guard would have analyzed more data. Moreover, he said, the Coast Guard would have conducted a sensitivity analysis of the estimate to determine how changes in the underlying assumptions would affect the size of the estimate. Analyzing uncertainty in this way is consistent with best practices for preparing benefit-cost analysis of significant regulatory actions called for by Executive Order No.12866, which applies to the Coast Guard's analysis.[36] For illustrative purposes, we conducted such an analysis and found that the Coast Guard's cost estimate of $7.3 billion could be more than $1 billion higher or lower, using generalized assumptions about cost uncertainty. That is, the estimate of $5.4 billion for securing facilities could range from $4.5 billion to $6.4 billion, and the estimate of $1.4 billion for securing vessels could range from $1.2 billion to $1.5 billion.

[36]A significant regulatory action is defined as likely to result in, among other things, a rule having an annual effect on the economy of $100 million or more or other serious effects. The Coast Guard has estimated that its rule for facilities and vessels will have an annual cost of $832 million in real, undiscounted dollars.

- **Questionable validity of some key assumptions**. The estimated $5.4 billion for securing facilities—the single biggest item—depends on key assumptions, which the Coast Guard has acknowledged are of questionable validity. For example, facilities are likely to vary in the extent to which they already have adequate security measures in place, and since no comprehensive data existed on the security preparations in place, Coast Guard officials had to make an educated guess about the extent of progress and the amount of additional security steps that would need to be taken. This is significant because the Coast Guard assumes facilities have already spent $17 billion on these security measures before MTSA requirements take effect. Thus, variation in these percentages can potentially have a sizable effect on costs. Another example is the Coast Guard also assumed that one-third of all facilities will have to spend about 60 percent more on security equipment than the remaining two-thirds of facilities will have to spend. However, some of the facilities in the lower-cost group will expand in the future to handle additional cargo resulting from economic growth, requiring more security and, therefore, placing more facilities than currently assumed in the higher-cost group. This can also have a substantial effect on costs. For example, assuming that 40 percent, rather than 33 percent, of all facilities fit in the higher-cost category, adds over $350 million to the costs of implementing these rules.

- **Limited span of time included in the analysis**. The Coast Guard's estimate covers a 10-year period beginning in 2003 and ending in 2012. However, MTSA security-related requirements are not limited to a 10-year period. Extending the period of analysis is also consistent with best practices for preparing economic analysis of significant regulatory actions called for by Executive Order No.12866.[37] Extending the Coast Guard's analysis by 10 years to 2022 raises the estimate of total costs by nearly 50 percent to $10.7 billion. Total costs continue to rise past 2012 because another $884 million in operation and maintenance, equipment replacement, and security guard costs are incurred with each additional year.[38]

- **Some potential costs not considered**. The Coast Guard's estimate does not include costs associated with possible delays in moving goods through more secure facilities, or account for higher prices for goods and services

[37]Guidance on implementing this executive order notes that the ending point of the analysis should be far enough in the future to encompass all the significant benefits and costs likely to result from the rule.

[38]The $884 million is in real, undiscounted dollars.

that could result if the maritime transportation industry tries to pass along higher security costs to its customers. For example, higher shipping rates could mean reduced water transportation services and reduced consumption and production of goods dependent on those services and associated economic losses.[39]

In the absence of complete data, the Coast Guard relied on public and stakeholder comments to determine if its estimate was valid. The Coast Guard held seven public meetings to discuss its estimate and said it received few negative comments. Given the limited time available, relying on such comments to identify large errors makes practical sense. There likely are limitations, however, in the extent to which the various stakeholders were in a position to comment on the validity of the estimate. For example, large cost differences between individual facilities or vessels could make it difficult to judge the accuracy of the Coast Guard's estimates of average facility or vessel costs.

The net effect of these limitations on the Coast Guard's estimate is unknown. However, it should also be pointed out that enhancing security could lower costs to society at large if implementing MTSA foils a terrorist attack and thereby prevents a costly disruption. For example, in 2002, U.S. ports handled $764 billion in international trade, or more than $2 billion per day. An event that disrupts this trade could have a substantial effect on the flow of goods, as well as a substantial impact on the larger economy.

Conclusions

The vulnerability of the nation's ports and the importance of addressing these vulnerabilities cannot be overemphasized. Since MTSA's enactment in November 2002, the Coast Guard has worked hard to address these vulnerabilities by spurring the development of meaningful security plans for thousands of facilities and vessels in the nation's ports. Progress has been made, though the extent to which all facilities and vessels will have adequate plans ready to implement as of July 1, 2004, is still unclear. This is particularly true for the thousands of self-certified plans. The Coast Guard has approved the guidelines and templates for these plans, but in most instances it has not seen the plans themselves.

As hard as the Coast Guard has worked to ensure that plans are developed, the most important part of the process still lies ahead because

[39]The net effect of these considerations on overall costs is unclear.

plans mean little if they do not actually produce better security. Many challenges lie ahead as the Coast Guard attempts to develop a complete picture of the security environment at the nation's seaports and take whatever actions are needed, when they are needed to protect those ports. The uncertainty about whether the Coast Guard will be able to meet its timeframes for conducting on-site compliance inspections of the more than 12,300 facilities and vessels and questions about whether it will have enough staff and a sufficient experience base to handle so many inspections will undoubtedly challenge management and staff to effectively implement the strategy. In addition, the complexity of compliance inspections that call for sophisticated judgments about vulnerabilities and the actions taken to address them will likely create the need for up-to-date training and guidance to help ensure that such decisions are thorough and consistent. During the initial surge period, these challenges make it important for the Coast Guard to carefully evaluate its efforts, so that problems or inadequacies can be identified. In the longer term, the Coast Guard can benefit from the lessons learned from this evaluation and use them to refine its long-term inspection strategy.

Several points stand out in particular as important in this evaluation effort.

- First, the inspection program the Coast Guard has established is an important feature of its strategy to improve port security. Having qualified inspectors is key to this effort. While the training the Coast Guard has adopted is an important step to build inspector skills and compensate for differences in their skills and experience, training alone does not provide assurance that those who conduct inspections are qualified. Nor does it substitute for policies on the professional development standards inspectors must meet. Filling these gaps takes on added significance given the criticality of inspectors' roles and the discretion they are anticipated to exercise.

- Second, the long-term strategy also needs to reflect a way to ensure that the security inspections assess conditions that represent the normal course of business at facilities and aboard vessels. One way to do this is to include conducting unscheduled and unannounced inspections and covert testing to provide additional information that, taken together with the results of annual compliance inspections, should provide better assurance that MTSA requirements are being implemented effectively.

Recommendation for Executive Action

To better ensure that MTSA requirements are being implemented effectively, we recommend that the Secretary of Homeland Security direct the Commandant of the Coast Guard to

- conduct a formal evaluation of compliance inspection efforts taken during the initial 6-month surge period, including the adequacy of security inspection staffing, training, and guidance, and use this evaluation as a means to strengthen the compliance process for the longer term. As part of this strategy, the Coast Guard should clearly define the minimum qualifications for inspectors and link these qualifications to a certification process. The Coast Guard should also consider including unscheduled and unannounced inspections and covert testing as part of its inspection strategy to provide better assurance that the security environment at the nation's seaports meets the nation's expectations.

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 generally agreed with the facts presented in the report and with the recommendation we made. The Coast Guard said our recommendation was reasonable and that the Coast Guard should certainly study its progress and make changes when necessary. Coast Guard officials also provided a number of technical clarifications, which we incorporated to ensure the accuracy of our report.

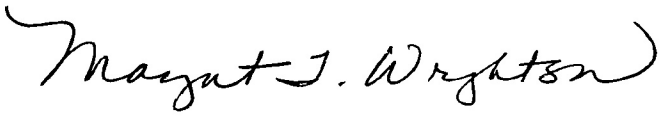
In its response, the Coast Guard raised one area where it disagreed with our presentation. This disagreement focused on how to characterize the Coast Guard's review of the Option B plans, which the Coast Guard refers to as "alternative security programs." The Coast Guard contended that its work on ASPs amounted to an approval of the plans themselves. The Coast Guard's comments in this regard were as follows:

"GAO states ASPs provide a 'template' and 'framework' for a plan, but not an actual plan. The ASPs were developed in the months leading up to the 31 December 2003 plan submission deadline, and hundreds of personnel-hours were spent working with the many industry associations used to ensure the template, when properly completed with appropriate details for a specific vessel/facility, would be a viable security plan to mitigate vulnerabilities for the vessel or facility type identified by the industry association. In fact, more hours were dedicated to each ASP than any individual plan, and as a result, the ASP templates produced a repeatable security plan precluding the need to have each completed template individually review by 1 July. Indeed, the CG considers them as approved security plans that must be implemented by 1 July. Primary burden is on the owners to comply with all applicable regulations. Our role is to ensure it is being done; 'Trust, but Verify'."

While we agree that the Coast Guard spent considerable time and effort reviewing and approving the templates and that this approach was understandable given the limited time available, we disagree with the Coast Guard's view that its actions should be considered as reviewing and approving the 5,900 individual Option B plans. The Coast Guard did not individually review and approve these plans; it reviewed and approved only the templates. The Coast Guard notes that Option B security plans would be viable only when "properly completed with appropriate details for a specific vessel/facility". Since the Coast Guard did not individually review the Option B plans; it does not know whether the plans have been properly completed.

This is more than a technical issue: We believe the distinction is important because the missing reviews add to the challenges the Coast Guard will face in its post-July 1 workload. The Coast Guard's extensive review of the 6,400 individual Option A plans found deficiencies in every single plan, raising concerns about how complete the 5,900 individual Option B plans are likely to be when Coast Guard inspectors arrive to conduct their inspections. Our discussions with Coast Guard officials and our visits to seven ports around the country provided indications that some owners and operators using Option B may not be fully aware of what they have to do to develop sufficient plans, or if they are aware of it, may be slow in complying. For example, the Coast Guard program manager stated that interactions with Option B users showed that some of them erroneously believed that membership in an industry or trade organization with approved standards and templates satisfied their obligation to implement a security plan. During our site visits, some port stakeholders told us that they were using Option B as a means to avoid preparing a security plan until July 1 while remaining in compliance with Coast Guard requirements. For all of these reasons, we chose not to change this aspect of our report.

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 IV. 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 first two objectives involved the security plans being developed for facilities and vessels. Specifically,

- assessing the progress made to develop, review, and approve the security plans for facilities and vessels by July 1, 2004.
- assessing the U.S. Coast Guard's monitoring and oversight strategy for ensuring that all necessary port security improvements are implemented.

We conducted a variety of work to assess key steps in the Coast Guard process for developing, reviewing, approving, and overseeing the implementation of security plans. These key steps in the process included the following:

- Identifying all the vessels and facilities that are subject to the requirement to develop plans.
- Ensuring that all identified parties have submitted plans for Coast Guard review.
- Reviewing all plans, identifying any deficiencies and ensuring their correction, and approving the completed plan.
- Establishing resources and an action plan to monitor implementation and compliance with requirements.

We carried out part of our work at Coast Guard headquarters or in consultation with headquarters officials. In this regard, we reviewed pertinent legislation, guidance, rules, and implementation documents to identify the purpose, objectives, process, enforcement strategy, and resources required to review and approve the security plans. We spoke with headquarters officials and reviewed relevant documentation to determine the management and methodology being used to address the implementation of the Maritime Transportation Security Act (MTSA). We met with MTSA's program manager and team to determine how they expected to review and approve the security plans before the July 2004 deadline, what resources and action plans are in place to oversee implementation after July 2004, what training program was needed to produce capable staff to perform inspections, how the staffing estimate for MTSA implementation was made, and what guidance would be provided to local inspectors and Captains of the Port to carry out MTSA implementation.

As part of our work in evaluating the process for reviewing security plans, we visited the Coast Guard's contractors at the Marine Safety Center in Washington, D.C., and the National Facility Security Plan Review Center in Overland Park, Kansas. During these visits, we also talked with contractor management and staff to determine how the review process worked, what reviewers were finding in the plans during their reviews, how deficient plans were dealt with, and what internal controls and quality assurance mechanisms were in place to ensure consistency during the review process. We also interviewed Coast Guard staff with the contractor staff at the review centers to determine the extent of their oversight roles and responsibilities in monitoring the contractors' performance.

We reviewed more site-specific planning and implementation activity through work conducted at seven specific maritime port areas. We selected these seven ports to provide a diverse sample of security environments and perspectives, basing our selections on such matters as geographic location, varying levels of strategic importance, and unique local characteristics. The seven ports and some of our reasons for choosing them are as follows:

- Corpus Christi, Texas: a Gulf Coast port that is a major port for military loadouts and important site for petroleum refining and chemical production.
- Huntington, West Virginia: a major inland river port and has a significant presence of critical chemical and petroleum producers.
- Los Angeles/Long Beach, California: the largest container port in the country.
- San Diego, California: a port that includes many military facilities and installations.
- Seattle/Tacoma, Washington: the third largest container traffic port in the country, and the port with the country's largest passenger ferry system.
- New Orleans, Louisiana: a large river port with many types of industrial and other facilities.
- New York, New York: another of the nation's largest container ports, and the site of the September 11th terrorist attacks.

During each of our visits to these seven ports we met with port stakeholders, Coast Guard marine safety offices, and Captains of the Port. The specific stakeholders we talked with at each port are listed in table 3. When we met with these stakeholders, we discussed the security assessments they had conducted, the facility or vessel security plans they were developing, any problems they had in developing those plans, and any assistance provided by the local Coast Guard during the process. When we met with Captains of the Port and marine safety offices, we discussed the extent to which they had identified all facilities and vessels under MTSA regulations within their port area, the outreach they provided to help stakeholders meet the statutory deadlines and understand MTSA requirements, the process they will use to ensure compliance after July 2004, and their general perspectives on MTSA requirements. We also attended several meetings put on by local marine safety offices, including a MTSA stakeholder forum, Area Maritime Security Committee (AMSC) meetings, and AMSC subcommittee meetings.

Table 2: Port Stakeholders GAO Contacted at Port Locations Reviewed

Port area	Stakeholders
Corpus Christi, Texas	United States Coast Guard Marine Safety Office Corpus Christi
	The Port of Corpus Christi
	Occidental Chemical Corporation
	Sherwin Alumina Company
	Valero Refining-Texas, LP
	Aransas-Corpus Christi Pilots
	Kirby Inland Marine, LP
	Union Pacific Railroad
	United States Bureau of Immigration and Customs Enforcement
	Boyd-Campbell Company
	Flint Hills Resources, LP
Huntington, West Virginia	United States Coast Guard Marine Safety Office Huntington
	West Virginia Department of Transportation, Public Port Authority
	Union Carbide Corp.
	Sunoco, Inc. (Haverhill, OH)
	American Electric Power (Columbus, OH)
	Bayer CropScience

Port area	Stakeholders
	Marathon Ashland Petroleum, LLC (Catlettsburg, KY)
	United States Army Corps of Engineers
	West Virginia Office of Emergency Services
	Kirby Inland Marine, LP
Los Angeles, California	United States Coast Guard Marine Safety Office Los Angeles/Long Beach
	The Port of Los Angeles
	The Port of Long Beach
	Marine Exchange of Southern California
	Long Beach Container Terminal, Inc.
	Crowley Marine Services, Inc.
	APL Limited
	Union Pacific Railroad
San Diego, California	United States Coast Guard Marine Safety Office San Diego
	Port of San Diego
	United States Navy
	California Highway Patrol
	San Diego Harbor Police
	National Steel and Shipbuilding Co.
	Continental Maritime
	San Diego Harbor Excursion
	United States Customs and Border Protection
Puget Sound, Washington	United States Coast Guard Marine Safety Office Puget Sound
	Port of Seattle
	Port of Tacoma
	Washington State Ferries
	Cruise Terminals of America
	Husky Terminal & Stevedoring, Inc.
New Orleans, Louisiana	United States Coast Guard Marine Safety Office New Orleans
	Port of New Orleans
	Port of South Louisiana
	Union Carbide Corporation
	Upper St. Rose Fleeting Co.
	Plaquemine Parish Ferry Department
	Zen-Noh Grain Corporation

Port area	Stakeholders
	Chalmette Refining, L.L.C.
	Shell Exploration and Production Company
	P & O Ports North America, Inc.
	United States Bureau of Immigration and Customs Enforcement
New York/New Jersey	United States Coast Guard Activities New York
	The Port Authority of New York & New Jersey
	General Chemical
	Staten Island Ferry System
	Lincoln Harbor Yacht Club
	Maersk, Inc.
	Howland Hook Container Terminal, Inc.
	Maher Terminals, Inc.

Source: GAO.

We also met with officials from industry trade groups such as the American Chemistry Council, American Association of Port Authorities, and the Association of American Railroads to determine their perception of MTSA requirements and the extent of interaction between port stakeholders and Coast Guard nationwide.

Finally, we followed-up with all the ports we visited to collect updated information on their respective progress in regard to our objectives. We then compared the information gathered through interviews and document analysis against pertinent criteria specified in MTSA, the final rule, and other Coast Guard guidance to determine the progress being made to develop vessel and facility maritime security plans and determine the sufficiency of Coast Guard resources and action plan to ensure that security plans are completed, reviewed, approved, and implemented in a timely manner.

Our third report objective was to determine the accuracy of the Coast Guard's estimates of the cost to comply with MTSA security planning and implementation requirements. To address this objective, we reviewed cost spreadsheets prepared by the Coast Guard documenting how cost estimates were developed. We identified key cost assumptions and the basis for the values assumed. Based on information about the basis for these assumed values, we conducted Monte Carlo simulations to determine the sensitivity of costs for facilities and vessels to generalized assumptions about cost uncertainty. As part of this review, we interviewed Coast Guard analysts responsible for these cost estimates. Besides

reviewing the cost spreadsheets, we reviewed documentation provided by the Coast Guard to support its choice of assumed values. We also asked Coast Guard officials responsible for these cost estimates what steps they took to ensure the reliability of the underlying data on which the estimates were based.

Our review was limited to security plans for facilities and vessels operating in domestic ports and did not include foreign ports, foreign flagged vessels, or the other security programs called for under MTSA.

We conducted our work from June 2003 to June 2004 in accordance with generally accepted government auditing standards.

Appendix II: Required Security Plan Items

Vessel security plans	Facility security plans
A vessel owner or operator must ensure that his or her plan consists of the individual sections listed below:	**A facility owner or operator must ensure that his or her plan consists of the individual sections listed below:**
(1) Security organization of the vessel.	(1) Security administration and organization of the facility.
(2) Personnel training.	(2) Personnel training.
(3) Drills and exercises.	(3) Drills and exercises.
(4) Records and documentation.	(4) Records and documentation.
(5) Response to change in MARSEC level.	(5) Response to change in MARSEC level.
(6) Procedures for interfacing with facilities and other vessels.	(6) Procedures for interfacing with vessels.
(7) Declarations of Security.	(7) Declaration of Security.
(8) Communications.	(8) Communications.
(9) Security systems and equipment maintenance.	(9) Security systems and equipment maintenance.
(10) Security measures for access control.	(10) Security measures for access control, including designated public access areas.
(11) Security measures for restricted areas.	(11) Security measures for restricted areas.
(12) Security measures for handling cargo.	(12) Security measures for handling cargo.
(13) Security measures for delivery of vessel stores and bunkers.	(13) Security measures for delivery of vessel stores and bunkers.
(14) Security measures for monitoring.	(14) Security measures for monitoring.
(15) Security incident procedures.	(15) Security incident procedures.
(16) Audits and Vessel Security Plan amendments.	(16) Audits and security plan amendments.
(17) Vessel Security Assessment Report.	(17) Facility Security Assessment Report.
	(18) Facility Vulnerability and Security Measures Summary (Form CG–6025).

Source: 33 C.F.R. 104.405 and 33 C.F.R. 105.405.

Appendix III: Analysis of Coast Guard's Compliance Cost Estimates

The Coast Guard estimated the maritime transportation industry will spend $7.3 billion to develop and implement security plans through the year 2012.[1] Of this amount, the estimate for owners and operators of facilities was $5.4 billion, and the estimate for owners and operators of vessels was $1.4 billion. The remainder—about $500 million—was for outer continental shelf facility and area maritime security and automatic identification system requirements. This appendix focuses on how the estimates for facilities and vessels were derived.

To make these estimates, the Coast Guard had to make a variety of assumptions about such matters as how many facilities and vessels would be affected, how extensive the planning and implementation efforts would have to be, and how much of a security framework was already in place that would go towards meeting MTSA requirements. The Coast Guard had to develop its estimates within a relatively short time, and it had limited amounts of data on which to base many of these assumptions. Factors that need to be kept in mind in considering the estimates include the uncertainties inherent in many of these assumptions, over what time period the costs were calculated, and the extent to which industry stakeholders had sufficient knowledge of their own to comment meaningfully on the Coast Guard's results.

Estimates Required Assumptions about Many Important Components

Several basic pieces of information were needed to compute the cost of developing and implementing security plans for facilities and vessels, and deriving these basic pieces of information involved making a variety of assumptions. The nation's ports and waterways are sprawling and diverse, and the facilities and vessels that are affected by MTSA requirements vary greatly in size and complexity. Facilities, for example, include not only port-operated docks and intermodal transfer stations, but also petrochemical facilities, power plants, and factories with hazardous materials. Developing the estimates involved making educated guesses about such things as how much effort they would have to expend on developing plans, what equipment and manpower would be called for in their plans, and how far along they already were.

[1]This estimate is based on costs to maintain security at MARSEC Level 1, which encompasses the Low (Green), Guarded (Blue), and Elevated (Yellow) designations of the Homeland Security Advisory System. The Coast Guard estimated that meeting a more extensive threat level, which the Coast Guard defined as two 21-day periods at MARSEC Level 2, the equivalent to the Department of Homeland Security's Advisory System's orange threat level (high risk of terrorist attack) each year, would cost an additional $5 billion.

Number of Facilities and Vessels

The Coast Guard first needed information on how many facilities and vessels would be affected by the regulation. The Coast Guard counted 4,965 facilities and 10,234 vessels affected by the regulation and assumed this tally would remain constant during the 10-year period of analysis from 2003 to 2012. According to the Coast Guard, these numbers were based on its Marine Safety Management System database, U.S. Army Corps of Engineer's waterborne statistics data, and a Department of Transportation database on ferries and terminals. The Coast Guard cited two previous studies to support its assumption that the number of facilities and vessels remain constant. First, in studying response plans for oil spills, the Coast Guard said it had found little yearly variation in facility numbers, because purchasing land and negotiating permits is time-consuming and prohibits significant numbers of facilities from entering and leaving the population. Second, in analyzing fire suppression on towing vessels, the Coast Guard reported very few vessels entering the domestic fleet, with the limited numbers largely being offset by vessels exiting the fleet.

Extent of Security Planning and Implementation Efforts

The Coast Guard next needed to determine how long it would take for facilities and vessels to complete security plans and what types of security measures they would need to take. Given the diversity of facilities and vessels, the Coast Guard assumed that some would require much more planning time and security measures than others. For facilities, the Coast Guard assumed that one-third of the total (1,638 of the 4,965 facilities) would require more time to draft security assessments and plans and would implement more security measures than the remaining 3,327 facilities. For example, the Coast Guard assumed that the 1,638 facilities would take 160 hours, on average, to draft security assessments and plans, compared with 80 hours for 3,327 other facilities.[2] Regarding the security measures that would need to be taken, the largest differences were in assumptions about the number of security guards. The Coast Guard tailored requirements for eight different facility types, such as container or break bulk facilities, hazardous substance facilities, and ferry and passenger terminals. For container or break bulk facilities, for example, the Coast Guard assumed that those facilities that had greater security needs would have 15 security guards, on average, compared with 4 security guards for those facilities with less extensive security needs.

[2]Not counting the number of hours spent annually on these documents.

Similarly, the Coast Guard assumed different types of vessels will require varying amounts of time to draft security assessments and plans and varying amounts of security measures. All told, the Coast Guard tailored security requirements by 26 vessel types. For these various types of vessels, the Coast Guard established estimates for the amount of planning time involved, the number of security personnel that would be needed, and average requirements for such security equipment as metal detectors, intrusion alarms, hand-held radios, locks, and lights. The Coast Guard also assumed nontowing vessels will need more security than towboats and barges and that companies with more than 10 vessels will need more security than companies with 10 or fewer vessels.

To establish many of these facility and vessel security requirements, the Coast Guard convened a self-described informal expert panel of economists, program managers, and other Coast Guard personnel with extensive field experience, including personnel currently stationed in field units. This group estimated the type and number of pieces of equipment and number of personnel required to comply with the requirements based on the type and configuration of a vessel or facility, locations of facilities, the average crew size aboard vessels, and how the Coast Guard envisioned vessels and facilities complying with the requirements. Because its requirements do not mandate specific equipment or personnel but set performance standards, the Coast Guard reported that it had to make broad assumptions about how industry would comply with these regulations.

Costs for Security Planning and Implementation

To translate the planning and implementation steps into a cost estimate, the Coast Guard also needed to establish assumptions about labor costs for each hour spent on security assessments and plans and costs per unit for each type of security measure. According to the Coast Guard, salaries for some personnel were based on previous analyses for salvage and marine firefighting and requirements for mechanical recovery and dispersants. Costs for security guards and other security personnel for facilities were based on national data from the Bureau of Labor Statistics along with a "loaded" labor factor to account for fringe benefits to these personnel. Equipment costs were based on product research and limited data received from industry during comment periods.

When these cost factors were applied, the results indicated that the one-third of facilities assumed to have more extensive planning and security needs would spend about 60 percent more on security equipment than the

lower-cost group. Similarly, spending for security equipment varied considerably between vessel types.

Extent to Which Adequate Security Measures Were Already in Place

Another important assumption deals with the extent to which facilities would already have security measures in place and, therefore, would not incur additional costs to comply with MTSA requirements. Among facilities, the Coast Guard assumed the level of prior investment varied substantially, both by type of facility and by type of equipment. According to the Coast Guard, many facilities, such as oil terminals, cruise terminals, and those dealing with hazardous materials, were already required to implement security measures under preexisting regulation by states or various federal agencies. Table 3 presents the Coast Guard's assumptions about the percentage of facilities that would need to purchase or enhance their security measures. For example, the Coast Guard assumed that most ferry terminals would need improvements with regard to gates, fencing, and number of security guards, but that no ferry terminals would need to improve their communications system.

Table 3: Coast Guard Assumptions about Extent of Prior Security Preparation

	Percentage of facilities needing to purchase or enhance security measures						
Type of facility	Communications system	Gates	Radio	CCTV	Lights	Fencing	Guards
Container or break bulk	5	30	5	5	5	5	30
Dry bulk	0	70	70	10	60	20	70
Hazardous bulk liquid	5	10	5	5	5	5	10
Hazardous substance (other)	5	5	5	5	5	5	5
Nonhazardous bulk liquid	10	10	10	10	10	10	10
Fleeting areas	5	0	5	10	0	0	10
Ferry terminals Group A	0	60	5	10	10	50	60
Ferry terminals Group B	0	80	5	10	10	50	80
Passenger terminals	5	5	5	5	5	5	5

Source: GAO analysis of Coast Guard data.

Many Assumptions Carry Limitations

Many of these assumptions carry limitations that need to be kept in mind in assessing the reliability of the estimate. For example, the assumptions reflected in table 3 above are based on incomplete data and a response rate from Coast Guard field units that the Coast Guard acknowledges seriously limit the reliability of any results. This is significant because the Coast Guard assumes facilities have already spent $17 billion on these security measures before MTSA requirements take effect. Thus, variations in the percentages shown in table 3 can have a potentially huge effect on costs. Actual costs to comply with the final rules could thus differ substantially from what the Coast Guard estimated because of simplifying assumptions that had to be made in the absence of complete data. In a number of cases, the Coast Guard cannot say if the value it assumed for a particular cost factor is the most likely one to occur, or likely to be too low or high.

Even relatively small changes in some of these assumptions can have a substantial effect on results. One example can be seen in changing the assumption about the percentage of facilities needing more extensive security measures. The Chief of the Standards Evaluation and Analysis Division said that some facilities would likely expand in the future to handle additional cargo resulting from economic growth. This expansion,

in turn, could require more security and potentially place more facilities than currently assumed in this higher-need group. For example, assuming that 40 percent of facilities should be in this higher-need group rather than the current 33 percent increases the cost estimate by over $350 million.

Limited Time to Estimate Costs Precluded More Extensive Data Collection and Analysis of Uncertainty

According to Coast Guard officials, the agency had only a matter of weeks to prepare its cost estimate, and the estimate had to be prepared without the benefit of extensive background research, vendor surveys, and field inventories. The Chief of the Standards Evaluation and Analysis Division, the Coast Guard official responsible for estimating costs, explained that had the Coast Guard more time they would have analyzed more data. Likewise, while the Coast Guard took the step of working with an expert panel, Coast Guard officials said this effort was not as extensive or sustained as under ideal circumstances. Time permitting, Coast Guard officials said, they would have convened an expert panel that included members of industry, nongovernmental organizations, and other government agencies, and this panel would have met multiple times over the course of many months, if not years.

Coast Guard officials also said that if time had permitted, they would have analyzed uncertainty in their estimate by conducting sensitivity or other analyses to determine how variations in these assumptions would change the cost estimate. Analyzing uncertainty in this way is consistent with best practices for preparing economic analysis of significant regulatory actions called for by Executive Order 12866, which applies to the Coast guard's analysis.[3] For illustrative purposes, we conducted a Monte Carlo analysis using the Coast Guard's cost models for facilities and vessels.[4] We found that the Coast Guard's cost estimate of $7.3 billion could be more than $1 billion higher or lower using generalized assumptions about cost uncertainty. This results from finding that the Coast Guard estimate of

[3]A significant regulatory action is defined as likely to result in, among other things, a rule having an annual effect on the economy of $100 million or more or other serious effects. The Coast Guard has estimated that its rule for facilities and vessels will have an annual cost of $832 million in real, undiscounted dollars.

[4]Our analysis was conducted using what is called Monte Carlo simulation, which uses random numbers to measure the effects of uncertainty. Because the Coast Guard was unable to provide additional information, our simulation is based on some general assumptions about the probability distributions characterizing values used by the Coast Guard for cost factors.

$5.4 billion to secure facilities could range from $4.5 billion to $6.4 billion, and its estimate of $1.4 billion to secure vessels could range from $1.2 billion to $1.5 billion.

Cost Estimate Spans Only 10 Years and Does Not Include All Costs

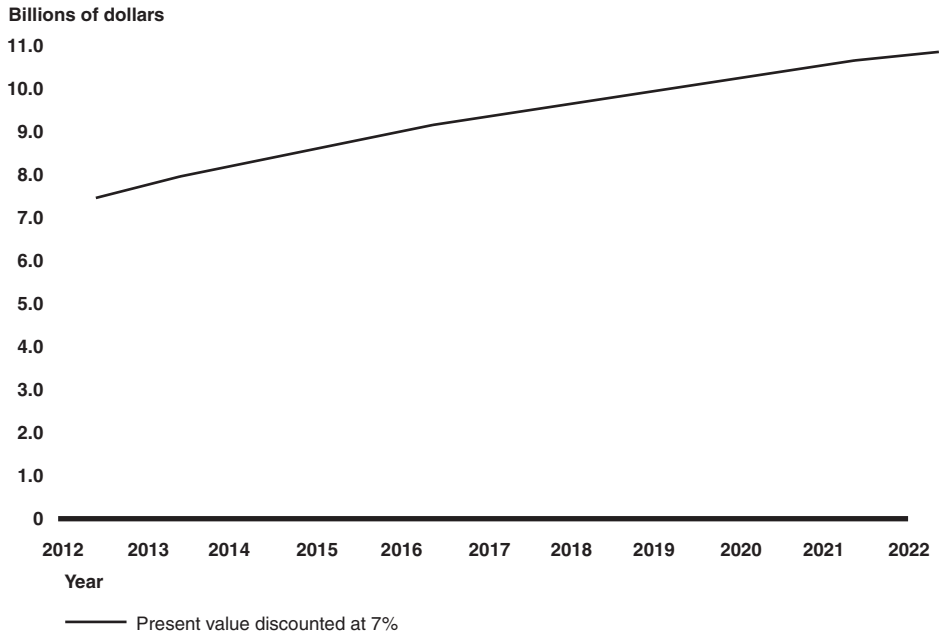
The Coast Guard has estimated it will cost $7.3 billion to develop and implement security plans from 2003 to 2012, but MTSA security related requirements are not limited to a 10-year period. Extending Coast Guard's analysis by 10 years to 2022 raises total costs by nearly 50 percent to $10.7 billion. Extending the period of analysis is consistent with best practices for preparing economic analysis of significant regulatory actions called for by Executive Order 12866.[5]

Figure 4 shows the trajectory of total costs as the time period of analysis is extended, holding the number of facilities and vessels constant. Total costs continue to rise past 2012 because another $884 million in operation and maintenance, equipment replacement, and security guard costs are incurred with each additional year.[6]

[5] Guidance on implementing this executive order notes that the ending point of the analysis should be far enough in the future to encompass all the significant benefits and costs likely to result from the rule.

[6] The $884 million is in real, undiscounted dollars.

Figure 4: Projection of Estimated Costs, 2012-2022



Source: GAO analysis.

The Coast Guard's estimate also does not include several types of costs:

- The estimate does not extend to costs beyond the maritime transportation industry. For example, it does not include costs associated with possible delays experienced by users in gaining access to more secure port facilities and the services they provide. It also does not include incremental costs borne by the Coast Guard to develop and enforce these new requirements.

- The estimate does not address higher prices for goods and services as the maritime transportation industry tries to pass along higher security costs to its customers. For example, higher shipping rates could mean reduced water transportation services and reduced consumption and production of goods and services dependent on those transportation services and associated economic losses.[7]

[7]The net effect of these considerations on overall costs is unclear.

- The Coast Guard has also estimated an additional $5 billion to meet an elevated threat level, which is not included in its $7.3 billion estimate.[8] It assumed a code orange alert occurs twice a year, with each elevated alert lasting 21 days. Increased personnel time is the primary cost. For example, vessel security officers and key crewmembers are assumed to work 16 hours per day during each elevation. For facilities, the number of security guards is doubled.

While the points noted above would add to the cost estimate, it should also be noted that other considerations could have the opposite effect. For example:

- Some facility and vessel owners may take steps to exempt themselves from the requirements, thereby lowering total costs. For example, some passenger vessel operators could elect to transport fewer people, placing their vessels into categories that do not have to comply with MTSA requirements. Other vessel operators could choose to no longer transport certain types of cargo and thus similarly become exempt. However, these mitigating actions on the part of vessel and facility owners may not be costless. For example, restrictive actions like those described may result in added costs to users of these transportation services.

- On the facilities side, companies will have an incentive to collaborate in designing collective security systems where opportunities exist to enhance security at less cost than if each company acted alone. For example, adjoining facilities may have opportunities to exploit possible cost economies in surveillance, access control, and communications. Moreover, because requirements to develop and implement security plans incorporate a performance-standard approach, there is flexibility in how a facility or vessel can comply, which could encourage lower-cost solutions than assumed by the Coast Guard. In addition, re-examining existing security arrangements as a result of the new requirements could lead to replacing some older, less cost-effective measures.

- Steps to enhance security could also lower costs to society at large if implementing security plans foils a security incident and prevents much larger costs. For example, in 2002, $764 billion in international trade was handled by U.S. ports, or more than $2 billion per day. Disruptions to this trade could have a large impact on the economy. In addition, security

[8]At MARSEC Level 2, which is the equivalent to the Department of Homeland Security's Advisory System orange level.

improvements from implementing security plans could have collateral benefits such as reducing nonsecurity related risks from theft and fire. Finally, if better security enhances demand for maritime transportation services, facility and vessel owners have positive incentives to comply.

Questions Remain about Adequacy of Public Comments to Validate Cost Estimate

In the absence of complete data, the Coast Guard relied on public comments to validate its cost estimate of $7.3 billion and ensure reliability of data used in that estimate. The extent to which the public comment process was up to this task is debatable. For instance, the Coast Guard acknowledged that on a vessel-by-vessel or facility-by-facility basis, its cost assumptions probably carry a large margin of error. Coast Guard analysts said the problem in estimating costs for facilities is that there is no typical facility. In turn, large cost differences for individual vessels and facilities could make it difficult for individual stakeholders to judge the accuracy of Coast Guard's estimates of average facility and vessel costs. In addition, the Coast Guard acknowledged that a key cost driver in the facility estimate—the national percentage of facilities requiring higher rather than lower costs to ensure security—is likely to rise over time. These issues call into question the adequacy of public comments to validate the estimate and ensure data reliability. However, given the limited time the Coast Guard had to gather data and make an estimate, relying on public comments to identify large errors made practical sense.

The Coast Guard vetted its cost estimate in seven public meetings and said it received few negative comments. For instance, some stakeholders commented that foreign-flag vessels should be included in the cost analysis, but, according to the Coast Guard, foreign-flag vessels are already required by the International Ship & Port Facility Security Code to meet these security requirements. On the other hand, the Coast Guard revised its cost values for portable vapor detectors and operations and maintenance for equipment after receiving comments that these values were too low. To help validate cost assumptions, the Coast Guard also established a proprietary docket where industry could provide it with cost data without worrying about disclosure in the public domain. However, not much data were submitted.

Appendix IV: 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, Geoffrey Hamilton, Christopher Hatscher, Nicholas Larson, and Stan Stenersen made key contributions to this report.

GAO's Mission

The General Accounting 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 the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone:
Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548