

GAO

Report to the Chairman, Committee on
Homeland Security, House of
Representatives

April 2010

MARITIME SECURITY

Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain



GAO

Accountability * Integrity * Reliability

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of [GAO-10-400](#), a report to the Chairman, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Over 9 million passengers departed from U.S. ports on cruise ships in 2008, and according to agency officials, cruise ships are attractive terrorist targets. GAO was asked to review cruise ship security, and this report addresses the extent to which (1) the Coast Guard, the lead federal agency on maritime security, assessed risk in accordance with the Department of Homeland Security's (DHS) guidance and identified risks; and (2) federal agencies, cruise ship and facility operators, and law enforcement entities have taken actions to protect cruise ships and their facilities. GAO reviewed relevant requirements and agency documents on maritime security, analyzed 2006 through 2008 security operations data, interviewed federal and industry officials, and made observations at seven ports. GAO selected these locations based on factors such as the number of sailings from each port. Results of the visits provided additional information on security, but were not projectable to all ports.

What GAO Recommends

GAO recommends that the Commissioner of Customs and Border Protection (CBP), the unified border security agency in DHS, conduct a study to determine whether requiring cruise lines to provide passenger reservation data to CBP would benefit homeland security, and if found to be of substantial benefit, determine the appropriate mechanism to issue this requirement. DHS concurred with our recommendation.

View [GAO-10-400](#) or [key components](#). For more information, contact Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

MARITIME SECURITY

Varied Actions Taken to Enhance Cruise Ship Security, but Some Concerns Remain

What GAO Found

The Coast Guard has assessed the risks to cruise ships in accordance with DHS guidance—which requires that the agency analyze threats, vulnerabilities, and consequences—and, with other maritime stakeholders, identified some concerns. Specifically, agency officials reported in January 2010 that there had been no credible threats against cruise ships in the prior 12 months, but also noted the presence of terrorist groups that have the capability to attack a cruise ship. The Coast Guard, cruise ship and facility operators, and law enforcement officials generally believe waterside attacks are a concern for cruise ships. Agency officials and terrorism researchers also identified terrorists boarding a cruise ship as a concern. The Coast Guard has also identified the potential consequences of an attack, which would include potential loss of life and economic effects.

Federal agencies, cruise ship and facility operators, and law enforcement entities have taken various actions to enhance the security of cruise ships and their facilities and implement related laws, regulations, and guidance, and additional actions are under way. DHS and component agencies have taken security measures such as the Coast Guard providing escorts of cruise ships during transit, and CBP's review of passenger and crew data to help target passenger inspections. Cruise ship and cruise ship facility operators' security actions have included developing and implementing security plans, among other things. The Coast Guard is also in the process of expanding a program to deter and prevent small vessel attacks, and is developing additional security measures for cruise ships. In addition, CBP's 2005-2010 Strategic Plan states that CBP should seek to improve identification and targeting of potential terrorists through automated advanced information. CBP, however, has not assessed the cost and benefit of requiring cruise lines to provide passenger reservation data, which in the aviation mode, CBP reports to be useful for the targeting of passengers for inspection. GAO's previous work identified evaluations as a way for agencies to explore the benefits of a program. If CBP conducted a study to determine whether collecting additional passenger data is cost effective and addressed privacy implications, CBP would be in a better position to determine whether additional actions should be taken to augment security.

Cruise Ship Escort by Coast Guard Boats



Source: U.S. Coast Guard.

Contents

Letter		1
	Background	5
	The Coast Guard Assesses Risk to Cruise Ships and Facilities in Accordance with DHS's Risk Assessment Guidance; Concerns Associated with Waterside Attacks Remain	13
	Stakeholders Have Taken Various Actions Pursuant to Laws, Regulations, and Guidance Designed to Enhance the Security of Cruise Ship Operations and Additional Actions Are Being Considered	19
	Conclusions	39
	Recommendation for Executive Action	39
	Agency Comments and Our Evaluation	40
Appendix I	Agency Comments	42
Appendix II	GAO Contact and Staff Acknowledgments	44
Related GAO Products		45
Tables		
	Table 1: Key International Stakeholders with Maritime Security Activities	7
	Table 2: Key Domestic Stakeholders with Maritime Security Responsibilities	8
	Table 3: Key International, National, and State Security Requirements Applicable to Cruise Ships	9
Figures		
	Figure 1: Leading U.S. Departure Ports and Destinations for North American Cruises in 2008	6
	Figure 2: Coast Guard Inspection of a Cruise Ship Facility	20
	Figure 3: Cruise Ship Escort by Coast Guard Boats	23
	Figure 4: Local Law Enforcement Vessel Enforcing a Security Zone	24

Figure 5: Truck Unloading Areas and Canine Screening of Stores
Awaiting Loading on Cruise Ship

Abbreviations

CBP	Customs and Border Protection
DHS	Department of Homeland Security
IMO	International Maritime Organization
ISPS	International Ship and Port Facility Security
MTSA	Maritime Transportation Security Act
SAFE Port Act	Security and Accountability For Every Port Act of 2006
TSA	Transportation Security Administration

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

April 9, 2010

The Honorable Bennie G. Thompson
Chairman
Committee on Homeland Security
House of Representatives

Dear Mr. Chairman,

Cruise ships are the single largest passenger conveyances in the world, with one ship currently in service that can carry more than 8,500 passengers and crew. The Coast Guard considers cruise ships to be highly attractive targets to terrorists, and according to a 2008 RAND Corporation report, cruise ships can represent high-prestige symbolic targets for terrorists. Moreover, terrorists have either targeted cruise ships or been able to board cruise ships in the past. The hijacking of the cruise ship Achille Lauro and killing of passenger Leon Klinghoffer by terrorists in 1985 was a watershed event for the cruise industry, leading to major changes in cruise line security procedures. More recently, in 2005, a plot to attack Israeli cruise ships off of the Turkish Mediterranean coast was discovered after the premature explosion of a bomb that was intended for the attack. A successful attack on a cruise ship in or near U.S. waters that resulted in the closure of a U.S. port or discouraged cruise travel would likely harm the U.S. economy because of the significant economic impact that ports contribute to the U.S. economy. For example, in a 2006 report, the Congressional Budget Office estimated that the closure of the ports of Los Angeles and Long Beach would reduce the U.S. Gross Domestic Product by up to \$150 million per day. Reduced demand for cruise travel following an attack could also have substantial economic effects as direct spending for goods and services by the cruise lines and their passengers in the United States was about \$19.1 billion in 2008.

Enacted after the September 11, 2001, attacks, the Maritime Transportation Security Act of 2002 (MTSA) places much of the responsibility for coordinating and overseeing maritime security efforts with the Department of Homeland Security (DHS).¹ Within the department, the U.S. Coast Guard is the lead federal agency responsible for a wide array of maritime safety and security activities including those

¹Pub. L. No. 107-295, 116 Stat. 2064 (2002).

involving cruise ships and facilities. Other U.S. government agencies, such as DHS's U.S. Customs and Border Protection (CBP), the unified federal agency responsible for border security, support the Coast Guard's maritime security mission by addressing a wide range of issues that affect international maritime commerce, including screening passengers arriving in the United States by cruise ship. State and local governments and the private sector also have responsibilities to secure domestic ports.

You requested that we identify threats and vulnerabilities—two elements of risk—associated with cruise ships and the measures being taken to protect them.² This report responds to the following questions:

- To what extent does the U.S. Coast Guard assess risk related to cruise ships and their facilities in accordance with DHS's guidance, and what are the identified risks?
- To what extent have maritime security stakeholders taken actions to mitigate the potential risks to cruise ships and their facilities and to implement applicable federal laws, regulations, and guidance, and what additional actions, if any, could enhance cruise ship security?

To determine the extent to which the U.S. Coast Guard assesses the risks related to cruise ships in accordance with DHS's guidance, and determine the identified risks associated with cruise ships and their facilities, we reviewed relevant federal guidance on the use of risk management, including the National Infrastructure Protection Plan.³ We also reviewed the Coast Guard's primary risk assessment tool, the Maritime Security Risk Assessment Model and Coast Guard documents describing the methodology and use of the risk assessment model. We analyzed the risk assessment model process and compared it to criteria with the risk assessment component of the National Infrastructure Protection Plan. We

²Risk assessment is a function of three elements: (1) threat—is the probability that a specific type of attack will be initiated against a particular target/class of targets, (2) vulnerability—the probability that a particular attempted attack will succeed against a particular target or class of targets, (3) consequence—the expected worst case or worse reasonable adverse impact of a successful attack.

³The National Infrastructure Protection Plan provides the unifying structure for the integration of critical infrastructure and key resources protection into a single national program. The plan provides an overall framework for programs and activities that are currently under way in the various industry sectors, as well as new and developing critical infrastructure and key resources protection efforts.

also analyzed the compiled nationwide results of the risk assessment model to determine the relative risks facing cruise ships and their facilities, as of July 2009. In addition, we interviewed Coast Guard headquarters personnel responsible for conducting comprehensive security reviews of critical maritime infrastructure with the risk assessment model, Coast Guard District personnel, and Coast Guard Sector personnel responsible for the implementation of the risk assessment model at the local level to discuss the relative risks in their areas of responsibility.⁴ We interviewed Coast Guard, Navy, and private sector intelligence personnel actively engaged in determining possible threats to cruise ships and their facilities. We also interviewed Coast Guard and CBP officials; personnel from five state and local law enforcement agencies; security personnel from five cruise lines and the Cruise Lines International Association, the key international cruise industry association; security personnel from nine cruise ship facility owners and operators (and one port authority with some security responsibility for a cruise facility) to determine their perspectives on the vulnerabilities of cruise ships and their facilities. The Coast Guard and CBP officials were those responsible for cruise ship and facility security at both the national level and at the locations where we made site visits. Similarly, the law enforcement personnel we met with represented jurisdictions covered in our site visits, and we also interviewed the facility owners and operators at those sites. We made these visits to a nonprobability sample of six cruise ship ports in the United States and four Coast Guard Sectors.⁵ We selected these locations based on the number of cruise ship sailings from the ports and the destinations for the cruise ship sailings. While the information we obtained from personnel at these locations cannot be generalized across all U.S. ports, it provided us with a perspective on the risks to cruise ship and facility security at the selected locations. The cruise lines we met with were primarily based on a nonprobability sample selected for their relative size and location. While their views may not represent views of all cruise lines, they do cover a substantial portion of the industry. For example, among members of the

⁴Coast Guard Sectors run all Coast Guard missions at the local and port level, such as search and rescue, port security, environmental protection, and law enforcement in ports and surrounding waters, and oversee a number of smaller Coast Guard units, including small cutters, small boat stations, and Aids to Navigation teams. Coast Guard Districts oversee Sectors, other Coast Guard units, such as Air Stations, and major buoy tenders.

⁵Our site visits were to ports in Fort Lauderdale and Miami, Florida; Long Beach and Los Angeles, California; San Juan, Puerto Rico; and Seattle, Washington. The Sectors we visited were Los Angeles-Long Beach, Miami, San Juan, and Seattle.

Cruise Lines International Association, the cruise lines we spoke with operate approximately 52 percent of vessels carrying 500 passengers or more in 2009.

To determine the extent to which maritime security stakeholders—including national and international governmental organizations, vessel owners, facility owners and operators, and law enforcement agencies—have taken actions to mitigate the potential risks to cruise ships and their facilities and to implement applicable federal laws and guidance, and determine what additional actions should be considered, we reviewed relevant federal legislation, regulations, and guidance. The scope of this review included MTSA; Security and Accountability For Every Port Act of 2006 (SAFE Port Act) amendments to MTSA;⁶ pertinent implementing regulations—such as 33 C.F.R. Parts 101, 102, 103, 104, 105; the Coast Guard’s Operation Neptune Shield operations order, Navigation and Vessel Inspection Circulars, and Maritime Security Directives, respectively. We analyzed data on the Coast Guard’s security performance in meeting internal standards established for Operation Neptune Shield during fiscal year 2008, and on cruise ship and facility operator’s security performance in meeting requirements identified in Coast Guard regulations, from 2006 to 2008. We found these data to be sufficiently reliable for the purpose of contextual or background information. To make this determination we conducted interviews with knowledgeable agency officials and performed data testing for missing data, outliers, and obvious errors. We also analyzed country reports from the Coast Guard’s International Port Security Program—which has responsibility for assessing the antiterrorism measures maintained by foreign ports—and Port Security Advisories to determine the level of security at major cruise ship foreign destinations. Although we reviewed CBP’s documents on passenger screening, such as the *Privacy Impact Assessment for the Automated Targeting System* and the *CBP Vessel APIS Guide*, and reviewed CBP’s objective to improve its identification and targeting of potential terrorists as stated in its 2005-2010 Strategic Plan, we did not conduct an independent evaluation of the Automated Targeting System. We also reviewed a prior GAO report discussing the use of program evaluations to identify benefits of federal programs. We interviewed federal officials from various agencies, including the Coast Guard and CBP to discuss their actions to reduce risks to cruise ships and their facilities. We observed security activities and interviewed state and local law enforcement

⁶Pub. L. No. 109-347, 120 Stat. 1884 (2006).

personnel and security personnel responsible for protecting cruise ships and their facilities from terrorist attacks at the ports we visited. While our observations at these locations cannot be generalized across all U.S. ports, it provided us with a general overview and perspective on cruise ship and facility security at the selected locations. We also made a site visit to one foreign cruise ship port to observe possible security actions other than those used in the United States. We selected this port because it was one of the few foreign cruise departure ports with many cruises to U.S. destinations.⁷

We conducted this performance audit from January 2009 to April 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Cruise Industry Carries Many Passengers and Has Numerous Sailings from U.S. Ports

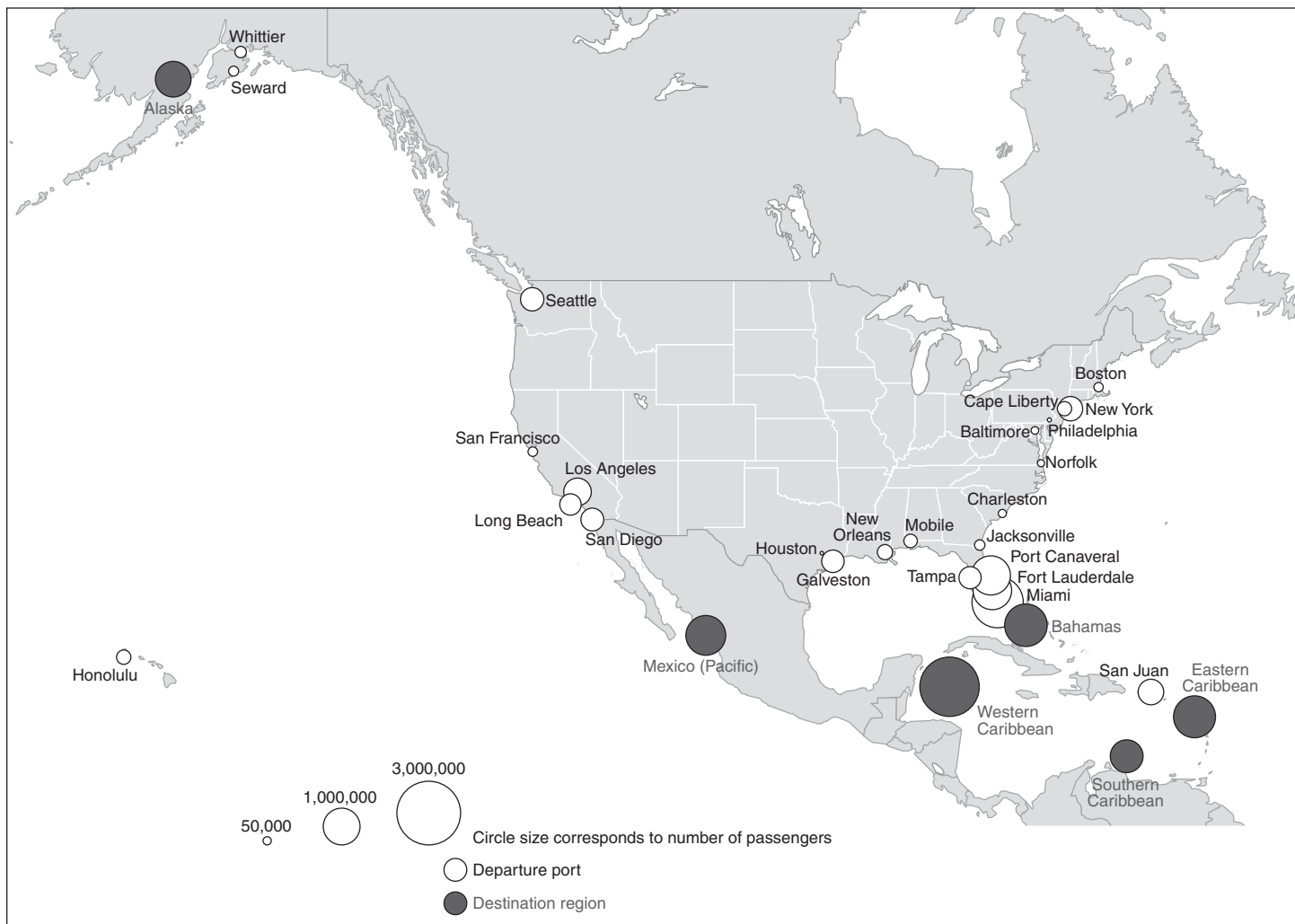
According to the Department of Transportation's Maritime Administration, over 9.3 million passengers departed from a U.S. port on North American cruises in 2008, on a total of almost 3,900 cruises from 30 ports.⁸ The U.S. ports with the most departures were located in Florida and include Miami, Fort Lauderdale, and Port Canaveral. Other ports with over 150 cruise departures in 2008 include Los Angeles, Long Beach, San Juan, and the New York City area. The Western Caribbean—including islands west of Haiti and ports in Mexico, Central America, and Columbia—was the most popular destination for passengers in 2008. These cruises carried nearly twice as many passengers, or more, than any other destination. Alaska, the

⁷The ports we visited account for approximately 56 percent of all cruise ship passengers and approximately 54 percent of North American cruises in 2008.

⁸Destinations for North American cruises include Alaska, Bahamas, Bermuda, Canada/New England, Eastern Caribbean, Hawaii, Mexico, nowhere (a cruise that does not call on any ports before it returns to its departure port), Pacific Coast, South America, South Pacific/Far East, Southern Caribbean, Trans-Panama Canal, Transatlantic, and Western Caribbean and include a U.S. port of call.

Bahamas, the Eastern Caribbean, and the Pacific coast of Mexico were other popular destinations in 2008. See figure 1 for a map showing leading North American cruise departure and destination ports, as well as the number of departing passengers for these ports.

Figure 1: Leading U.S. Departure Ports and Destinations for North American Cruises in 2008



Sources: GAO analysis of US Customs and Border Patrol data; cruise line data; and the Official Steamship Guide International.

Many Stakeholders Involved in Securing Cruise Ship Operations

Numerous international and domestic organizations play a role in the security of cruise ships. The non-U.S. stakeholders are diverse and have wide-ranging roles and responsibilities. These stakeholders include international organizations, governments of nations where cruise ships make stops or are registered, and owners and operators of the vessels and facilities (see table 1).

Table 1: Key International Stakeholders with Maritime Security Activities

Organization or agency	Key maritime security-related activities
International organizations	
<ul style="list-style-type: none"> International Maritime Organization (IMO) The International Maritime Organization is a specialized agency of the United Nations with 169 member states that is responsible for developing an international regulatory framework addressing, among other things, maritime safety and security. 	<ul style="list-style-type: none"> Responsible for developing and maintaining a comprehensive regulatory framework for shipping. Responsible for developing international standards for port and vessel security.
<ul style="list-style-type: none"> Cruise Lines International Association Cruise Lines International Association is composed of 25 cruise lines that represent 97 percent of the cruise capacity marketed from North America. 	<ul style="list-style-type: none"> Responsible for acting as the coordinating body and conduit of information for its members in meetings with U.S. security agencies at the national level.
Overseas governmental agencies	
<ul style="list-style-type: none"> Designated Authorities Agencies of IMO member governments or their representatives responsible for implementing international maritime security requirements. In the United States, the designated authority is the U.S. Coast Guard. 	<ul style="list-style-type: none"> Responsible for setting security levels at a country's ports. Responsible for reviewing vessel and facility security plans and overseeing compliance with these plans.
International private sector	
<ul style="list-style-type: none"> Vessel owners, operators, and crew; and terminal operators 	<ul style="list-style-type: none"> Responsible for implementing vessel security plans that meet relevant security standards.

Source: GAO.

In addition to international stakeholders, there are various domestic maritime security stakeholders in the United States. Table 2 lists key federal agencies and other domestic stakeholders, together with examples of the maritime security activities they perform.

Table 2: Key Domestic Stakeholders with Maritime Security Responsibilities

Stakeholders	Key maritime security-related responsibilities
Federal government: Department of Homeland Security	
<ul style="list-style-type: none"> U.S. Coast Guard 	<ul style="list-style-type: none"> Conduct vessel escorts, boardings of selected vessels, and security patrols of key port areas. Ensure vessels in U.S. waters comply with domestic and international maritime security standards. Review U.S. vessel and facility security plans and oversee compliance with these plans. Meet with foreign governments and visit foreign port facilities to observe security conditions.
<ul style="list-style-type: none"> U.S. Customs and Border Protection (CBP) 	<ul style="list-style-type: none"> Prior to a vessel arrival in the United States, screen information on its history, crew, passengers, and cargo for items that would lead to further examination. Review documentation of all persons, baggage, and cargo arriving from foreign ports. Ensure that all have appropriate documents to gain access to the United States. Take action to deny admissibility of aliens to the U.S., or take other appropriate enforcement action based on the results of the border search. Operate the National Targeting Center that analyzes information used to target persons for additional screening.^a
<ul style="list-style-type: none"> Transportation Security Administration (TSA) 	<ul style="list-style-type: none"> Test technologies, practices, and techniques for passenger screening systems in the maritime environment. Coordinate with the Coast Guard on security training and surge operations.
State and local governments	
<ul style="list-style-type: none"> Law enforcement agencies 	<ul style="list-style-type: none"> Often act as land-based security for facility operators. If agency operates a marine unit, support Coast Guard role through water patrols and possibly escorts.
<ul style="list-style-type: none"> Port authorities 	<ul style="list-style-type: none"> Own many cruise ship facilities and responsible for ensuring their security.
Private sector	
<ul style="list-style-type: none"> Vessel owners and operators 	<ul style="list-style-type: none"> Develop and implement vessel security plans that meet applicable laws and regulations.
<ul style="list-style-type: none"> Security contractors 	<ul style="list-style-type: none"> Provide security services at cruise ship facilities.
<ul style="list-style-type: none"> Facilities contractors 	<ul style="list-style-type: none"> Operate some cruise ship facilities on behalf of owners.

Source: GAO.

^aThe National Targeting Center is a multiagency operations center that conducts national level targeting and analysis in support of border-related efforts to identify and interdict terrorists through reports on individuals entering the country at land, sea, and airports.

Maritime Security Actions Are Guided by Legal and Regulatory Framework

International, national, and state and local requirements guide maritime security, including the security of cruise ships and their facilities. At the international level, the International Maritime Organization (IMO), through its International Ship and Port Facility Security (ISPS) Code, a part of the International Convention for the Safety of Life at Sea, lays out the international framework designed to help ensure maritime security.⁹ National laws, regulations, and guidance direct federal agencies and vessel and facility operators on a nationwide basis. State and local requirements may also further direct activities of operators within their jurisdictions (see table 3).

Table 3: Key International, National, and State Security Requirements Applicable to Cruise Ships

Promulgator	Law or guidance	Key provisions
International		
IMO	International Ship and Port Facility Security (ISPS) Code, ^a as implemented through Chapter XI-2 of the International Convention for the Safety of Life at Sea ^b	Sets out many of the international standards for vessel and port facility security. For example, all covered vessels shall have a designated security officer.
United States		
U.S. federal government	Maritime Transportation Security Act of 2002 (MTSA) ^c	Establishes a maritime security framework including many of the U.S. vessel and port facility security requirements and standards and for Coast Guard enforcement of many of such provisions. One such provision, for example, facilities and vessels that may be in a transportation security incident shall have vulnerability assessments.
	SAFE Port Act amendments to MTSA (2006) ^d	Sets additional requirements for Coast Guard regulation of port facility security. For example, at least one security inspection—an inspection of a facility to verify the effectiveness of its security plan—of regulated facilities shall be unannounced.
	Immigration and Nationality Act (1952) ^e	Section 235 of the Immigration and Nationality Act and implementing regulations provide for the examination of all persons seeking to enter the U.S. by a CBP officer. Once determined not to be a citizen or national of the United States the applicant will be inspected as an alien. All aliens are subject to inspection to determine the admissibility of all individuals seeking to enter the United States.

⁹Adopted by IMO's Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, the ISPS Code establishes requirements for contracting governments of countries where ports are located, contracting governments of countries where ships are registered, operators of port facilities, and operators of vessels traveling on the high seas.

Promulgator	Law or guidance	Key provisions
	Intelligence Reform and Terrorism Prevention Act of 2004 ^f	Requires information about passengers and crews on cruise ships to be compared to watch lists to prevent suspected or known terrorists and their associates from boarding, or to subject them to additional security scrutiny.
Coast Guard	Implementing Regulations (such as 33 C.F.R. Parts 101, 104, and 105)	Based on legislative authority, set specific security requirements for U.S. flagged vessels and port facilities. For example, owners or operators of cruise ships shall ensure the screening of all persons, baggage, and personal effects for dangerous substances and devices.
	Operation Neptune Shield operations order	Sets internal Coast Guard standards for vessel (including cruise ships) security activities, which include escorts and security boardings—boardings performed to verify the information submitted in advance of the ship’s arrival, verify that the ship and crew are operating as expected, and to act on intelligence that may have prompted security concerns. For example, Coast Guard units are required to escort a certain percentage of high capacity passenger vessels—those carrying 500 or more passengers—under different Maritime Security levels. ^g (Specific percentages are classified.)
	Navigation and Vessel Inspection Circulars	Provide guidance about the enforcement of or compliance with certain federal maritime regulations and Coast Guard maritime safety programs. For example, how Coast Guard inspectors are to ensure compliance with international safety and security standards on foreign cruise ships.
	Maritime Security Directives	Set security performance standards for stakeholders responsible for taking security actions commensurate with various Maritime Security levels. For example, one standard includes the various percentages of vessel stores that need to be inspected under different Maritime Security levels.
State Government: Florida	Seaport security legislation (2000)	At the state level, for example, Florida law requires the development and implementation of port security plans in Florida. ^h

Source: GAO.

^fIMO Doc. SOLAS/CONF. 5/34 (Dec. 12, 2002).

^g32 U.S.T. 47, T.I.A.S. No. 9700.

^hPub. L. No. 107-295, 116 Stat. 2064 (2002).

ⁱPub. L. No. 109-347, 120 Stat. 1884 (2006).

^jPub. L. No. 82-414, 66 Stat. 163 (1952).

^kPub. L. No. 108-458, 118 Stat. 3638 (2004).

^lMaritime Security levels are a three-tiered threat warning system to provide a means to easily communicate preplanned scalable responses to increased threat levels. They are set to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the United States.

^mFla. Stat. tit. 22 § 311.12(3).

The enforcement of security requirements aimed at vessels is governed by two different systems: flag state control and port state control. The flag state is the country in which the vessel is registered and flag state control can generally extend anywhere in the world that the vessel operates. A flag

Risk Management Is Important
for Cruise Ship and Facility
Security

state that is a contracting government to International Convention for the Safety of Life at Sea has responsibility for ensuring that vessels flying its flag meet international security standards and that such flag state's standards be at least as stringent as those included in the convention's ISPS Code. The port state is the country where the port is located. Port state control is the process by which a nation exercises its authority over foreign-flagged vessels operating in waters subject to the port state's jurisdiction. Port state control is generally intended to ensure that vessels comply with various international and domestic requirements for ensuring safety of the port, environment, and personnel. Thus, when a foreign-flagged cruise ship enters U.S. waters or a U.S. port, the U.S. port state control program, administered by the U.S. Coast Guard, becomes an additional means of maritime security enforcement. According to an official of the Cruise Lines International Association, of the cruise lines included in our site visits, only one had a vessel registered in the United States. Hence, although they carry large numbers of U.S. passengers, the vast majority of cruise line-operated vessels generally come under U.S. authority only when they enter waters over which the United States has jurisdiction.

Risk management plays an important role in homeland security. Because the United States cannot afford to protect itself against all risks, Congress has charged DHS with coordinating homeland security programs through the application of a risk management framework.¹⁰ In 2006, DHS issued the National Infrastructure Protection Plan, which is DHS's base plan that guides how DHS and other relevant stakeholders should use risk management principles to prioritize protection activities within and across each critical infrastructure sector in an integrated and coordinated fashion.¹¹ Updated in 2009, the National Infrastructure Protection Plan requires that federal agencies use this information to inform the selection of risk-based priorities and the continuous improvement of security

¹⁰For more information on how DHS and the Coast Guard utilized risk management for port security, see GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, [GAO-06-91](#) (Washington, D.C.: Dec. 15, 2005).

¹¹Critical infrastructure are systems and assets, whether physical or virtual, so vital to the United States that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Homeland Security Presidential Directive 7 divided up the critical infrastructure in the United States into 17 industry sectors, such as transportation, energy, and communications, among others. In 2008, under authorization of Homeland Security Presidential Directive 7, DHS established an 18th sector—Critical Manufacturing.

strategies and programs to protect people and critical infrastructure by reducing the risk of acts of terrorism.

Within the risk management framework, the National Infrastructure Protection Plan also establishes baseline criteria for conducting risk assessments. According to the National Infrastructure Protection Plan, risk assessments are a qualitative and/or quantitative determination of the likelihood of an adverse event occurring and are a critical element of the National Infrastructure Protection Plan risk management framework. Risk assessments can also help decision makers identify and evaluate potential risks so that countermeasures can be designed and implemented to prevent or mitigate the potential effects of the risks. The National Infrastructure Protection Plan characterizes risk assessment as a function of three elements:

- **Threat:** The likelihood that a particular asset, system, or network will suffer an attack or an incident. In the context of risk associated with a terrorist attack, the estimate of threat is based on the analysis of the intent and the capability of an adversary; in the context of a natural disaster or accident, the likelihood is based on the probability of occurrence.
- **Vulnerability:** The likelihood that a characteristic of, or flaw in, an asset's, system's, or network's design, location, security posture, process, or operation renders it susceptible to destruction, incapacitation, or exploitation by terrorist or other intentional acts, mechanical failures, and natural hazards.
- **Consequence:** The negative effects on public health and safety, the economy, public confidence in institutions, and the functioning of government, both direct and indirect, that can be expected if an asset, system, or network is damaged, destroyed, or disrupted by a terrorist attack, natural disaster, or other incident.

Information from the three elements that assess risk—threat, vulnerability, and consequence—can lead to a risk characterization and provide input for prioritizing security goals. For example, MTSA required the Coast Guard to prepare Area Maritime Security Plans for ports around the United States. These plans convey operational and physical security measures, communications procedures, timeframes for responding to security threats, and other actions to direct the prevention of and response to a security incident. In its regulations implementing MTSA, the Coast Guard gave the primary responsibility for creating the Area Maritime

Security Plans primarily to the Captain of the Port, based on the Area Maritime Security Assessment.¹² Area Maritime Security Assessments examine the threats and vulnerabilities to activities, operations, and infrastructure critical to a port and the consequences of a successful terrorist attack on the critical activities, operations, and infrastructure at the port. Under the regulations, such assessments are to be risk-based, and assess each potential threat and the consequences and vulnerabilities for each combination of targets and attack modes in the area. With the information supplied in the assessment, the Area Maritime Security Plan is to identify, among other things, the operational and physical security measures to be implemented at Maritime Security Level 1 and those that, as risks increase, will enable the area to progress to levels 2 and 3.

The Coast Guard Assesses Risk to Cruise Ships and Facilities in Accordance with DHS's Risk Assessment Guidance; Concerns Associated with Waterside Attacks Remain

Risk Assessment

The Coast Guard uses a tool, known as the Maritime Security Risk Analysis Model, to assess risk for various types of vessels and port infrastructure, including cruise ships and cruise ship facilities, which is in accordance with the guidance on assessing risk from DHS's National

¹²The Captain of the Port is the Coast Guard officer designated by the Commandant to enforce within his or her respective areas port safety and security and marine environmental protection regulations, including, without limitation, regulations for the protection and security of vessels, harbors, and waterfront facilities.

Infrastructure Protection Plan. The Coast Guard uses the analysis tool to help implement its strategy and concentrate maritime security activities when and where relative risk is believed to be the greatest. The model assesses the risk—threats, vulnerabilities, and consequences—of a terrorist attack based on different scenarios; that is, it combines potential targets with different means of attack, as recommended by the risk assessment aspect of the National Infrastructure Protection Plan.¹³ Examples of a Maritime Security Risk Analysis Model scenario related to cruise ships include a truck bomb or a boat attack. According to the Coast Guard, the model’s underlying methodology is designed to capture the security risk facing different types of targets, allowing comparison between different targets and geographic areas at the local, regional, and national levels. Also in accordance with National Infrastructure Protection Plan, the model is designed to support decision making for the Coast Guard. At the national level, the model’s results are used for (1) long-term strategic resource planning, (2) identifying capabilities needed to combat future terrorist threats, and (3) identifying the highest-risk scenarios and targets in the maritime domain. For example, Coast Guard officials reported that results are used to refine the Coast Guard’s Operation Neptune Shield requirements for the number of required cruise ship escorts and patrols of cruise ship facilities. At the local level, the Captain of the Port can use the model as a tactical planning tool. The model can help identify the highest risk scenarios, allowing the Captain of the Port to prioritize needs and better deploy security assets. As we reported in March 2009, Intelligence Coordination Center officials stated that the Coast Guard uses the model to inform allocation decisions, such as the deployment of local resources and grants.¹⁴

Risk to Cruise Ships and Their Facilities

Although in January 2010 intelligence officials working at the National Maritime Intelligence Center stated there has been no credible terrorist threat against cruise ships identified in at least the preceding 12 months, stakeholders generally agreed that waterside attacks are a concern for

¹³The Coast Guard Intelligence Coordination Center quantifies threat as a function of intent (the likelihood of terrorists seeking to attack), capability (the likelihood of terrorists having the resources to attack), and presence (the likelihood of terrorists having the personnel to attack).

¹⁴For more information on risk assessment models used in the aviation transportation mode, see GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, [GAO-09-492](#) (Washington D.C., March 27, 2009).

cruise ships, and if attacks were successfully carried out, they could have extensive consequences. Despite the lack of evidence identifying recent threats, maritime intelligence officials identified the presence of terrorist groups that have the capability to attack a cruise ship, even though they have not identified any intent. As we previously reported in 2007, security officials in the U.S. government are concerned about the possibility of a future terrorist attack in a U.S. port.¹⁵ For example, captured terrorist training manuals cite ports as targets and instruct trainees to use covert means to obtain surveillance information for use in attack planning. Terrorist leaders have also stated their intent to attack infrastructure targets within the United States, including ports, in an effort to cause physical and economic damage, and inflict mass casualties. In addition, as reported both by the Coast Guard and RAND, cruise ships have been terrorist targets in the past and are still considered attractive targets for terrorists.¹⁶ Although intelligence officials reported that there have been no recent threats against cruise ships, this does not preclude the possibility of such an incident occurring in the future.¹⁷

According to maritime stakeholders, some concerns regarding cruise ship security exist, particularly with respect to waterside security. According to the Coast Guard's Strategy for Maritime Safety, Security, and Stewardship, one of the greatest risks associated with maritime scenarios is a direct attack using waterborne improvised explosive devices. Officials we interviewed from the Coast Guard's Intelligence Coordination Center stated that waterside attacks are a concern for cruise ships. Similarly, DHS's Small Vessel Security Strategy states that small vessels could be used as a waterborne improvised explosive device to attack maritime targets as they have in the past overseas.¹⁸ The strategy further states

¹⁵GAO, *Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers*, [GAO-08-141](#) (Washington, D.C., Dec. 10, 2007).

¹⁶Reports that discuss a terrorist attack on a cruise ship include Michael D. Greenberg, Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz, *Maritime Terrorism: Risk and Liability* (Santa Monica, Calif., 2006); and United States Coast Guard, *The U.S. Coast Guard Strategy for Maritime Safety, Security, and Stewardship* (Washington, D.C., 2007).

¹⁷Although intelligence officials reported no credible threats against cruise ships, some stakeholders stated that they had experienced potential threats such as incidents involving false bomb threats, suspicious items, or the identification of a prohibited item on board a cruise ship.

¹⁸Department of Homeland Security, *Small Vessel Security Strategy* (Washington, D.C., April 2008). Additional information on the strategy is included later in this report.

that cruise ships operate in areas that are frequented by small vessels which may easily blend or disappear into other vessel traffic in ports and the coastal maritime environment, and are usually subject to less scrutiny than larger vessels in these areas.

Coast Guard personnel from all of the four Sectors and 18 of the 25 port security stakeholders we interviewed also stated that a waterside attack is one of the most significant concerns for cruise ships.¹⁹ At one port we visited, various stakeholders responded to reports of a small vessel operating within the security zone of a cruise ship in 2007. Although the stakeholders cleared the cruise ship for departure after searching the area around the ship and its hull with divers, the small vessel was able to get within close proximity of the cruise ship before stakeholders responded. Representatives from the Cruise Lines International Association also reported that the greatest security concern for cruise ships is a waterside attack.

Waterside attacks can also occur while a cruise ship is in transit, such as when pirates in the Gulf of Aden and western Indian Ocean attacked cruise ships. For example, at least three cruise ships have been attacked by pirates on small boats while armed with automatic weapons and rocket propelled grenades. The three vessels were able to evade the pirates by either maneuvering or fighting back. Some cruise line officials we interviewed stated that they decided not to sail to places where security risks exist, but as of 2009, some continue to sail in the Gulf of Aden. One cruise ship operator we interviewed stated that the passengers who take cruises that sail in these areas tend not to be Americans and are people who are comfortable with risk. This official told us that they explain the level of risk to the passengers and their strategy for minimizing the risk.

According to officials at the National Maritime Intelligence Center there is also a concern that a terrorist could get on board a cruise ship to carry out a terrorist attack. For example, in 1985, terrorists were able to board and hijack a cruise ship, the Achille Lauro, resulting in the death of a passenger. Since that attack, various additional security measures have been implemented; including screening of passengers, crew members, and their baggage. However, according to a 2006 RAND report on maritime

¹⁹Of the seven stakeholders who did not mention waterside attacks, five reported either being comfortable with the level of law enforcement presence at their port or being more concerned about other threats, such as criminal acts of smuggling and drug trafficking at their port.

terrorism, if terrorists were successful in gaining access to a cruise ship, once on board, they could carry out various attack scenarios.

Coast Guard officials and some port security stakeholders reported that concerns also exist for cruise ship facilities at U.S. and foreign ports. Personnel from two of the four Sectors and 6 of the 25 port security stakeholders we interviewed mentioned a vehicle borne explosive at a cruise ship facility as a concern, and 5 of the 25 port security stakeholders we interviewed mentioned concern about the possible risk of an armed individual attacking others at a cruise ship facility.²⁰ Further, 6 port security stakeholders expressed concerns about the security level at some foreign ports, although Coast Guard reports from foreign port site visits indicate that there are few concerns with foreign ports that cruise ships typically call upon. Specifically, six recent reports from the Coast Guard's International Port Security Program²¹ indicate that these countries, which include some of the most frequent cruise ship destinations, are generally found to be compliant with the ISPS Code. As part of the program's activities, the Coast Guard also recommends changes that could improve security at cruise ship facilities in some locations as a result of their visits to these locations. In addition, although the Coast Guard's October 2009 Port Security Advisory identifies 13 countries that are not maintaining effective anti-terrorism measures, a representative from the Cruise Lines International Association stated that these countries are not typical destinations for the cruise lines that the association represents.

A successful attack on a cruise ship could affect the ship, its passengers, and the U.S. economy. As a result of an attack, damage to the cruise ship

²⁰These scenarios are not exclusive to a cruise ship facility, but rather any location where people are congregated.

²¹The International Port Security Program has responsibility for assessing the antiterrorism measures maintained by foreign ports. In response to MTSA provisions directing DHS to assess the effectiveness of antiterrorism measures maintained by foreign ports, which are served by vessels that also call on the United States, the Coast Guard established the International Port Security Program. A staff based in Washington, D.C. sets program policy and makes determinations regarding the effectiveness of antiterrorism measures. An operational element based in Portsmouth, VA and Liaison Officers in three regions (Asia-Pacific, Europe/Africa/Middle East, and Central/South America, for worldwide coverage) conduct country visits to review and discuss security measures implemented and share best practices in order to assist other nations and facilitate bilateral exchanges. A Port Security Specialist Team based in Washington, D.C. was established to manage country visits to review and discuss security measures implemented and share "best practices." According to Coast Guard officials, during country visits, not all ports are visited by program officials.

could occur and the extent of the loss of life would depend on the severity of the attack, according to various studies.²² Coast Guard officials stated that cruise ships are built to sustain various types of attack scenarios and keep passengers safe until they are able to be rescued, and that a very large hole in the hull would have to occur to cause any significant damage to the ship. Furthermore, according to the 2006 RAND study, most experts agree that sinking a cruise ship would be extremely difficult. However, according to this report and intelligence officials, the economic consequences of an attack on a cruise ship could be significant, as a successful attack on a cruise ship could result in decreased demand for cruise vacations, affecting a multibillion dollar industry. The RAND report further states that all attack modes targeting cruise ships have comparable estimates of potential economic harm. However, parasitic bombings—which involve a diver placing a highly explosive device on the hull of the ship, ramming attacks with improvised explosive devices, and biological attacks, including those involving contamination of a ship’s food or water supply, are projected to present greater potential for human casualties.

²²The Coast Guard has conducted studies on the impacts of different types of attacks on cruise ships, the results of which are classified.

Stakeholders Have Taken Various Actions Pursuant to Laws, Regulations, and Guidance Designed to Enhance the Security of Cruise Ship Operations and Additional Actions Are Being Considered

Stakeholders' Actions

In their efforts to secure cruise ships and their attendant port facilities, the responsible stakeholders—including the Coast Guard, CBP, Transportation Security Administration (TSA), DHS, as well as cruise ship owners and cruise ship facility operators—have taken various actions to implement applicable key maritime federal laws, regulations, and guidance designed to help ensure the security of cruise ships and cruise ship facilities.

The Coast Guard conducts multiple types of security activities. The Coast Guard engages in both regulatory and operational activities designed to secure cruise ships and their facilities. As part of its regulatory activities, the Coast Guard inspects cruise ship facilities and cruise ships to ensure that they are meeting security requirements.²³ Under SAFE Port Act amendments to MTSA, the Coast Guard is required to conduct security inspections of MTSA-regulated maritime facilities, including cruise ship facilities, at least twice a year to verify the effectiveness of the facilities' security plans, and one of these inspections must be conducted without

²³The Coast Guard performs other annual and periodic vessel inspections that are primarily focused on safety, during which security measures are also reviewed.

prior notice to the facility.²⁴ During our observations of two cruise ship facility inspections, Coast Guard inspectors reviewed the security plan, checked to ensure that guards were at designated access points, and questioned facility personnel on security procedures. See figure 2 for a photograph depicting a Coast Guard inspection of a cruise ship facility.

Figure 2: Coast Guard Inspection of a Cruise Ship Facility



Source: U.S. Coast Guard.

²⁴Under Coast Guard guidance, a Coast Guard inspector must carry out the following steps in conducting a cruise ship facility inspection: (1) ensure the facility complies with the security plan; (2) ensure the approved security plan adequately addresses the performance-based criteria as outlined in federal regulations; (3) ensure the adequacy of the security assessment; and (4) ensure that the measures in place adequately address the vulnerabilities.

In addition to the inspection of cruise facilities, to enforce security and safety provisions under international agreements, domestic legislation and Coast Guard guidance, the Coast Guard also inspects cruise ships entering U.S. ports.²⁵ Coast Guard guidance states that cruise ships are subject to security inspections as determined necessary by a risk-based targeting process to ensure that cruise ships are complying with security regulations and conventions.²⁶ Vessels that have not been inspected in the last 12 months are subject to an inspection upon port arrival under this targeting process. Coast Guard officials stated that security examinations on high-capacity passenger vessels can be both announced and unannounced. Coast Guard officials stated that there are systems in place to identify when cruise ships and cruise ships facilities are due for inspection.²⁷ Coast Guard officials stated that the Captain of the Port is responsible for ensuring that all cruise ship facilities inspections are conducted by reviewing the appropriate systems data. With respect to cruise ship inspections, Coast Guard officials stated that, at the time of our review, the agency exceeded the total number of required cruise ship security inspections. In February 2008, we reported that although Coast Guard officials told us that field units were meeting their inspection requirements for facilities, inspections may not have been documented in the Coast Guard's database, or inspections may have been delayed by staff being diverted to meet higher-priority needs.²⁸ Coast Guard officials stated that

²⁵Under Coast Guard guidance, the Coast Guard should determine if a cruise ship is complying with maritime security requirements through observation, asking questions, and reviewing security records. If there is evidence that the ship does not meet the applicable maritime security requirements, the Coast Guard can impose enforcement actions that include inspection, delay, or detention of the ship; restriction of ship operations; expulsion of the ship from port; and/or lesser administrative or corrective measures. According to Coast Guard guidance, a foreign flagged cruise ship's security plan is not generally subject to inspection, and the Coast Guard must obtain consent from the ship's flag state or the master of the ship before reviewing the ship's security plan.

²⁶The Coast Guard utilizes a screening tool that promotes systematic evaluation of several risk factors related to a ship's compliance or noncompliance with domestic and international maritime security standards. The risk factors are: ship management; flag state; recognized security organization; the vessel's security compliance history; and the ship's last ports of call.

²⁷For cruise ships entering a U.S. port, the Coast Guard uses a targeting system to determine whether the ship is required to receive an inspection. A Coast Guard database allows Coast Guard units to run a report on a daily basis for all facilities. The report highlights which facilities are due for an inspection.

²⁸GAO, *Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data*, [GAO-08-12](#) (Washington, D.C., Feb. 14, 2008).

they are taking steps to rectify these issues by redesigning the database system to make it easier for the user to input data, which they expect to complete by 2011. In addition, they have created a daily report to inform local Coast Guard units when each facility is due for an inspection. Coast Guard officials stated that the agency is reviewing options on how to use its database as a method for headquarters to better track the local units' performance in meeting their inspection requirements.

The Coast Guard has also taken various operational actions designed to secure cruise ships. Through its internal guidance, the Coast Guard sets the standards for local Coast Guard units to meet for security activities, such as conducting passenger vessel escorts or security boardings. For example, Operation Neptune Shield requires Coast Guard units to escort a certain percentage of high capacity passenger vessels while in transit. These vessels include cruise ships, ferries, and excursion vessels carrying 500 or more passengers.²⁹ Coast Guard data on Operation Neptune Shield performance shows that some districts did not meet their requirements for high capacity passenger vessels escorts in fiscal year 2008; however, Operation Neptune Shield allows the Captain of the Port the latitude to shift resources to other priorities when deemed necessary, for example, when resources are not available to fulfill all missions simultaneously.³⁰ See figure 3 for a photograph of a Coast Guard boat escorting a cruise ship.

²⁹The required percentage of escorts changes at different threat levels. The Coast Guard can coordinate with local law enforcement to assist with meeting its Operation Neptune Shield requirements for escorting vessels.

³⁰The Coast Guard collects Operation Neptune Shield data on all high-capacity passenger vessels, but does not separate the data by type of high-capacity passenger vessel, such as cruise ships or ferries.

Figure 3: Cruise Ship Escort by Coast Guard Boats



Source: U.S. Coast Guard.

Another Coast Guard security action involves security boardings of cruise ships. Such security boardings are done to verify the information submitted in advance of the ship's arrival; verify that the ship and crew are operating as expected; and to act on intelligence. In 2008, the Coast Guard conducted pre-entry security boardings on some, but not all, cruise ships at major U.S. ports.³¹ According to Coast Guard officials, these boardings were conducted because these cruise ships met certain criteria under the Coast Guard's targeting process.³²

By regulation and at the discretion of the Captain of the Port, Coast Guard units, with or without the assistance of local law enforcement, may partake in other security measures as well. One such security measure is the enforcement of security zones that require other vessels to remain a

³¹More specific information on the number of security boardings the Coast Guard conducts is considered security sensitive information.

³²The Coast Guard uses a classified, risk-based tool to evaluate the security risk of a vessel entering into port, and determine whether a boarding is deemed appropriate. The tool helps Coast Guard units to determine the appropriate actions to be taken for a cruise ship, such as an inspection or boarding.

certain distance from cruise ships. During our site visits to the ports, we observed the enforcement of security zones. See figure 4 for a photograph depicting a local law enforcement vessel enforcing a security zone at a port. The Coast Guard also partakes in waterborne, airborne, and shoreside patrols of critical infrastructure and key resources, including cruise ship facilities. In addition to its regulatory and operational activities to protect cruise ships and their facilities in the United States, the Coast Guard's International Port Security Program also reviews port security conditions in foreign ports and recommends actions and measures to improve the antiterrorism measures in use at such ports, pursuant to MTSA requirements.

Figure 4: Local Law Enforcement Vessel Enforcing a Security Zone



Source: GAO.

CBP reviews passenger and crew lists for terrorist and criminal connections. CBP also maintains a role in the security of cruise ships and their facilities by screening passengers and crew for terrorist connections or criminal ties, and by helping to ensure that all passengers and crew are

cleared for entry into the United States.³³ Under CBP's implementing regulations, operators of commercial vessels such as cruise ships are required to provide CBP with advance lists of information on passengers and crew—also known as a manifest.³⁴ Before a cruise ship departs or arrives in the United States, CBP checks these manifests to screen persons against certain databases, such as terrorist watchlists and the National Crime Information Center database, to determine their potential risk to the United States or the cruise ship. This screening process identifies individuals with potential terrorism links or criminal warrants, as well as identifies those passengers and crew with potential immigration admissibility problems, among other things.³⁵ For example, at one port we visited, we observed CBP officers removing a passenger from a cruise ship, due most likely to an outstanding criminal warrant, according to agency officials. For those cruise ships arriving in the United States, the agency also reviews the manifest to determine passenger and crew admissibility into the United States. Admissibility inspections are performed to determine the nationality and identity of each person wishing to enter the United States and for preventing the entry of ineligible aliens, including those thought to be criminals, terrorists, or drug traffickers. In the case of cruises originating at Canadian ports for U.S. destinations, CBP officials stated that CBP checks the admissibility of all

³³Under the Intelligence Reform and Terrorism Prevention Act of 2004, for cruise ships on an international voyage that embarks or debarks passengers at a U.S. port, DHS is to compare information about cruise ship passengers and crew with consolidated database information relating to known or suspected terrorists and their associates.

³⁴Under CBP regulations, cruise ships are required to transmit arrival manifest data at least 96 hours before entering the U.S. port or place for voyages of 96 hours or more; prior to departure of the ship from a foreign port for voyages less than 96 but at least 24 hours; or at least 24 hours before entering the United States place or port for voyages of less than 24 hours. In addition, ships are required to submit manifest data 60 minutes before departure from the United States. Manifest data requirements include, among other things, full name, date of birth, gender, citizenship, country of residence, status on board the ship, travel document type, passport information (if required), address while in the United States (not required for U.S. citizens, lawful permanent residents, crew members, or persons who are in transit to a location outside the United States), voyage information, and ship information.

³⁵In general, with respect to Coast Guard's maritime security regulations, the term "screening" is defined to mean "a reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers, and crew. The purpose of the screening is to secure the vital government interest of protecting vessels, harbors, and waterfront facilities from destruction, loss, or injury from sabotage or other causes of similar nature. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present."

passengers prior to the cruise ship departing Canada.³⁶ Finally, agency officials reported that they inspect all passengers and crew before they enter into the United States when they disembark cruise ships, including those passengers whom CBP inspected while in Canada.³⁷

TSA primarily has a supporting role. TSA's role in cruise ship security is primarily as an advisor on transportation security screening and technologies. The agency also coordinates with the Coast Guard on security training and port security surge operations. TSA officials stated that the agency has conducted explosives and radiation screening technology pilot programs for passenger vessels and facilities, which include cruise ships, as part of its Security Enhancement and Capabilities Augmentation Program. Designed specifically for the maritime environment, TSA documents state that the program gives TSA the opportunity to network with different ferry and cruise ship operators around the United States, test emerging technologies, and develop strategies that the agency can use to respond to specific threats that arise from new intelligence or major events. Since February 2003, TSA officials stated that the agency has visited over 12 venues to test new technologies for screening passengers, ships, baggage, and stores to be loaded on passenger vessels, and that the goal of the pilot programs is to determine how the technologies work in different environments and in large scale application. The Security Enhancement and Capabilities Augmentation Program pilots can also provide operators with justification for grant funding, according to TSA. The pilots also give local agencies opportunities to observe and try the technologies. TSA officials stated that TSA shares the results of its pilots with the Cruise Lines International Association and cruise ship facility operators, including both pilot participants and nonparticipants. Although TSA does not track cruise ship facility operators that have implemented new technologies as a result of the TSA screening pilots, TSA officials reported that five facility operators, which included cruise ship operators, have adopted new technologies as a

³⁶CBP officers conducting admissibility inspections for passengers boarding U.S.-bound cruise ships in Canada are permitted by informal agreement with Canadian authorities to check bags or do pat downs. However, according to Customs and Border Protection officials, taking any action beyond that would necessitate coordination with local Canadian law enforcement.

³⁷Crew that are denied landing privileges by a CBP officer while in the United States are regularly mustered for compliance in the port of arrival and onward U.S. ports. CBP also notifies other federal and local law enforcement of detained crew for situational awareness.

result of a TSA pilot program. TSA officials stated that TSA also creates and distributes security training courses for passenger vessel employees. The courses address topics to improve employees' security awareness, increase the effectiveness of their reactions to suspicious items and persons, and assist in their efforts to respond to a transportation security incident. According to TSA officials, the agency's involvement in surge operations is primarily through its Visible Intermodal Prevention and Response program. The program's deployments involve the use of the agency's assets, including explosive detection capabilities, transportation security officers, Federal Air Marshals and behavior detection officers—to help enhance the security of any transportation mode. Officials stated that since 2006 there have been 180 Visible Intermodal Prevention and Response maritime deployments.

DHS developed a strategy to address the small vessel threat. DHS released the Small Vessel Security Strategy in April 2008 as part of its effort to mitigate the vulnerability of vessels—including cruise ships—to waterside attacks from small vessels, and the implementation plan for the strategy is under review. According to the strategy, its intent is to reduce potential security and safety risks posed by small vessels through operations that balance fundamental freedoms, adequate security, and continued economic stability. The goals of the Small Vessel Security Strategy are to (1) develop and leverage a strong partnership with the small vessel community and public and private sectors; (2) enhance maritime security and safety; (3) leverage technology to enhance the ability to detect, determine intent, and when necessary, interdict small vessels; and (4) enhance coordination, cooperation, and communications between federal, state, local, and tribal stakeholders, the private sector, and international partners. Subsequent to the development of the strategy, DHS began drafting a plan to implement the goals of its strategy. In January 2010, a DHS official stated that the implementation plan was currently awaiting approval by the Deputy Secretary of DHS, after which it would need to be sent to the Office of Management and Budget for review. Subsequent to the Office of Management and Budget's approval, the implementation plan would be released. In September 2009, DHS's Office of Inspector General produced a report that identified concerns with the Small Vessel Security Strategy and the draft version of its implementation plan. According to the report, while DHS had made progress in responding to potential small vessel threats, more remained to be done to provide effective guidance and operate effective programs to address small vessel

threats.³⁸ In addition, the Office of Inspector General recommended that DHS develop a more comprehensive strategy by (1) addressing the desirable characteristics and elements missing from its strategy and draft implementation plan and (2) evaluating the effectiveness of programs intended to support small vessel security before including them as part of its solution to improve security against the small vessel threats.³⁹ DHS partially concurred with the Office of Inspector General's first recommendation and plans to address this recommendation in the execution of its implementation plan. DHS did not concur with the Office of Inspector General's second recommendation to evaluate the effectiveness of programs intended to support small vessel security, stating that the agencies that submitted specific actions for the implementation plan had already considered their effectiveness to support small vessel security.

Cruise ship and facility operators implemented various security actions on board cruise ships and at facilities. Pursuant to the ISPS Code and its guidance, and Coast Guard's implementing MTSA regulations and guidance like other regulated vessels and facilities, cruise ship and cruise ship facility operators must develop and implement security plans that address vulnerabilities identified in their security assessments. ISPS-regulated cruise ship and cruise ship facility operators are also required to ensure security assessments are completed and inspections are conducted to ensure they are meeting security requirements. Under Coast Guard regulations specifically directed to cruise ship facility operators, cruise ship facilities must meet additional security requirements, such as implementing measures to screen all persons, bags, and personal effects for dangerous substances and devices; check the identification of all persons trying to enter the facility; designate holding, waiting, or embarkation areas within the facility's secure area to segregate screened persons and their personal effects from unscreened persons and their personal effects; and provide additional security personnel to designated

³⁸DHS Office of Inspector General, *DHS' Strategy and Plans to Counter Small Vessel Threats Need Improvement*, OIG-09-100, (Washington, D.C.: September 10, 2009).

³⁹The Office of Inspector General report concluded that DHS incorporated two characteristics of an effective national strategy for combating terrorism—(1) purpose, scope, and methodology and (2) problem definition and risk assessment. However, the report stated that DHS had not fully addressed the remaining four characteristics—(1) goals, objectives, activities, and performance measures; (2) resources, investments, and risk management; (3) organizational roles, responsibilities, and coordination; and (4) integration and implementation.

holding, waiting, or embarkation areas within the facility's secure area, among other things. Similarly, cruise ship operators, under Coast Guard regulations specifically directed to cruise ships, must also meet additional security requirements, including the screening of all persons, bags, and personal effects for dangerous substances and devices; checking the identification of all persons attempting to board the cruise ship; and performing security patrols. To address such requirements in their security plans, stakeholders reported using various measures such as the presence of security guards or local law enforcement, and the use of cameras, vehicle checkpoints, canines, access control measures, and dive teams.⁴⁰ See figure 5 for a photograph depicting truck unloading areas and canine screening of stores to be loaded onto a cruise ship. Cruise ship and cruise ship facility operators may use local law enforcement and security contractors to help meet security requirements. We also observed security contractors conducting passenger screening and noted the presence of local law enforcement at the facilities during a port visit.

⁴⁰Under MTSA, a security plan for U.S. vessels and facilities must (1) be consistent with the requirements of the National Maritime Transportation Security Plan and Area Maritime Transportation Security Plans; (2) identify the qualified individual having full authority to implement security actions, and require immediate communications between that individual and the appropriate federal official and the persons providing personnel and equipment; (3) include provisions for—establishing and maintaining physical security, passenger and cargo security, and personnel security; establishing and controlling access to secure areas of the vessel or facility; procedural security policies; communications systems; and other security systems; (4) identify, and ensure by contract or other means approved by the Secretary of DHS, the availability of security measures necessary to deter to the maximum extent practicable a transportation security incident or a substantial threat of such a security incident; (5) describe the training, periodic unannounced drills, and security actions of persons on the vessel or at the facility, to be carried out under the plan to deter to the maximum extent practicable a transportation security incident, or a substantial threat of such a security incident; (6) be updated at least every 5 years; and (7) be resubmitted for approval of each change to the vessel or facility that may substantially affect the security of the vessel or facility. Under Coast Guard regulations, the Coast Guard is to review and approve security plans for U.S. flagged vessels and facilities. A foreign flagged vessel's security plan, under Coast Guard regulations, is generally not subject to Coast Guard review, approval, or inspection.

Figure 5: Truck Unloading Areas and Canine Screening of Stores Awaiting Loading on Cruise Ship



Source: GAO.

Although the Coast Guard has identified security-related deficiencies for cruise ship facilities and cruise ships, agency officials stated that cruise ship and cruise ship facility operators generally maintain good security measures. Of the over 1,900 cruise ship facility inspections the Coast Guard conducted in calendar years 2006 through 2008, Coast Guard data show 347 deficiencies recorded for all cruise ship facilities.⁴¹ Coast Guard officials stated that cruise ship facilities tend to have more requirements than other types of port facilities but also tend to better implement security measures, and that most deficiencies are corrected at the time of the inspection.⁴² Officials further stated that there was a decline in the number of cruise ship facility deficiencies in 2008, indicating that these facility operators have a better understanding of SAFE Port Act requirements. Personnel from the four Sectors we met with had issued few enforcement actions against cruise ship facilities in 2008—with one of the four Sectors issuing three letters of warning against a cruise ship facility

⁴¹Inspection data do not include domestic cruise ship facilities that typically cannot support a cruise ship as defined by MTSA. These facilities may handle gaming vessels or dinner cruises.

⁴²Other port facilities include boat ramps, bulk liquid and oil facilities, and container facilities.

for concerns related to access control.⁴³ Of the over 1,500 foreign cruise ship vessel inspections the Coast Guard conducted in calendar years 2006 through 2008, Coast Guard data shows 18 security-related deficiencies for foreign cruise ship operators. Violations were generally related to issues with the cruise ship's access control or restricted areas. Coast Guard officials stated that cruise ship vessel deficiencies tend to be less significant than those for other vessel types, and attributed this to the seriousness in which cruise ship operators approach security and the fact that these operators have a professional staff dedicated to security duties. Officials we interviewed from the four Coast Guard Sectors we visited stated that they had not issued any enforcement actions against a cruise ship in 2008, although personnel from one Sector stated that it had to delay a cruise ship because of a document violation.

Furthermore, federal officials and cruise ship operators we interviewed reported that cruise lines implemented security measures beyond what is required of them. Federal officials, including Coast Guard officials, told us that because of the significant impact that a cruise ship attack could have on the industry, the cruise lines are very serious about security. The five cruise ship operators we interviewed all stated that their daily security operations are comparable to what the Coast Guard requires at elevated threat levels. According to cruise ship operators, the actions taken by cruise ship operators to ensure security include making risk-based decisions regarding which ports to call on, whether to conduct additional screening on board ships at foreign ports, whether to require foreign governments to take additional actions to secure their ports, and providing their own security protocols at their private ports of call. Specifically, cruise ship operators stated that they have cancelled planned destinations because of security conditions in some locations. According to these operators, these decisions have been triggered by various factors such as the heightened security concerns following the November 2008 terrorist attack in Mumbai, India, piracy activity in the Gulf of Aden, and intelligence reports.

Stakeholders reported using various coordination efforts. As part of their efforts to secure cruise ships and their facilities, representatives from the Coast Guard, Cruise Lines International Association, and other port security stakeholders reported using various coordination efforts

⁴³A letter of warning is issued for minor first-time violations that operators take immediate action to correct.

including meetings, jointly operated command centers, and the Coast Guard's HOMEPORT—a secure Internet communications portal between Coast Guard Sectors and the port stakeholders in their areas of responsibility. Specifically, stakeholders reported participating in the Area Maritime Security Committee meetings, security officer meetings, and Cruise Lines International Association security meetings⁴⁴. According to Cruise Lines International Association representatives, the association has hosted regular security meetings every 60 days for over 10 years, and coordinates with several intelligence agencies for these meetings, including the Federal Bureau of Investigation, Office of Naval Intelligence, the Department of State's Overseas Security Advisory Council, Coast Guard, and CBP. Furthermore, Cruise Lines International Association representatives stated that most of the security directors for the cruise lines are former military or law enforcement officers, who bring established contacts and relationships in the security and intelligence fields with them to the private sector. Personnel from all four Coast Guard Sectors and all 25 port security stakeholders we met with generally reported positive relationships among the stakeholders. Four of the 25 stakeholders, however, mentioned some challenges working with federal agencies. For example, 1 stakeholder stated that initially there was some uncertainty about who had authority to make decisions about cruise ship operations, the Coast Guard or CBP, but that it had become clearer over time.

Coast Guard Is Considering Additional Actions

The Coast Guard has plans to implement new maritime security awareness efforts to enhance the security of cruise ship operations. One of these efforts is intended to mitigate the threat posed by a small vessel attack. According to federal agencies, the U.S. government has limited information on recreational vessels, and it is difficult to detect a small vessel attack without prior intelligence. DHS documents state that the U.S. government has incomplete knowledge of the recreational boating public, their travel patterns, and the facilities they use, and that identifying and

⁴⁴Area Maritime Security Committees established under Coast Guard's MTSA implementing regulations, in addition to the local Coast Guard Captain of the Port, may be composed of officials of federal, territorial, or tribal government; state and local government; law enforcement and security organizations; maritime industry and labor organizations; and other port stakeholders that either may be affected by security practices and policies or have a special competence in maritime security. The responsibilities of the committees include, in part, identifying critical port infrastructure, identifying risks to the port, developing mitigation strategies for these risks, and communicating appropriate security information to port stakeholders.

distinguishing legitimate small vessel users from those with intent to harm is difficult. Further, Coast Guard and Navy studies have demonstrated challenges in stopping a small vessel attack once one is under way. As we reported in March 2009, given the number of potential threats in many areas and the short period of time in which to respond to a threat, thwarting an attack by a smaller vessel without advance knowledge of the threat may prove challenging even with available systems and equipment that track smaller and noncommercial vessels in coastal areas, inland waterways, and ports.⁴⁵ According to one Coast Guard official, the ISPS Code contributes to the overall security of vessels but is not specifically aimed at preventing a small vessel attack. However, the Coast Guard provides armed interdiction capability that when present helps to deter small vessel attacks, according to this official. The concern about small vessel attacks is exacerbated by the fact that most cruise ships sail according to precise schedules and preplanned itineraries that are readily available through the Internet, advertising brochures, or travel agents. As a result, information that could provide valuable intelligence for terrorists is easily obtained, allowing an attacker to pick the time and place to prepare for and carry out an attack against a targeted cruise ship.

To address the waterside small vessel threat nationally, the Coast Guard has piloted a new initiative to enhance public awareness called Operation Focused Lens. Operation Focused Lens is a Coast Guard District-level initiative to increase awareness of suspicious activity in and around U.S. ports. It complements Operation Neptune Shield by helping to identify, deter, and prevent a small vessel attack, and directs additional resources and effort toward gathering information about the most likely points of origin for an attack, such as marinas, landings, and boat ramps. A Coast Guard District official stated that Operation Focused Lens had minimal impact on cost and resources, as they were able to easily shift resources to meet the requirements of Operation Focused Lens. According to Coast Guard officials, the Coast Guard views Operation Focused Lens to be a best practice, and the agency is considering plans to integrate Operation Focused Lens into its community awareness program, America's Waterway Watch, and is developing requirements to implement aspects of Operation Focused Lens at additional locations. Coast Guard officials

⁴⁵GAO, *Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should Be Reviewed*, [GAO-09-337](#) (Washington, D.C., March 17, 2009).

stated that they plan to discuss the expansion of Operation Focused Lens at the April 2010 Operation Neptune Shield conference.

The Coast Guard also plans to develop new security regulations for cruise ships by 2011 in response to recommendations regarding cruise ship security measures made by the National Maritime Security Advisory Committee in 2006. The advisory committee was established under authority of MTSA to provide advice to the Secretary of Homeland Security via the Commandant of the Coast Guard on matters such as national security strategy and policy, actions required to meet current and future security threats, international cooperation on security issues, and security concerns of the maritime transportation industry. In 2006, the Coast Guard asked advisory committee members to specifically review and make recommendations regarding cruise ship security measures. The advisory committee's recommendations included: (1) developing and publishing a listing of prohibited items not allowed on board cruise ships; (2) developing equipment performance standards for screening detection equipment; and (3) developing standards for screening operations, training, and qualifications of persons engaged in screening activities at cruise ship facilities.

Coast Guard officials stated that in an effort to address the National Maritime Security Advisory Committee's recommendation, a Notice of Proposed Rule Making for Cruise Ship Security Measures is under development with a publication date expected in 2011. Coast Guard officials stated the rule making will propose regulations that will provide detailed, flexible requirements for the screening of persons, baggage and personal items intended for boarding a cruise ship, and that they are working in consultation with TSA and the National Maritime Security Advisory Committee. Given the actions taken by the Coast Guard and port security stakeholders to protect cruise ships and their facilities from terrorist attacks, Coast Guard officials stated that aside from its planned actions, there are no additional measures that it should take or take more broadly at this time to protect cruise ships, as the current layered security practices included in vessel and facility security plans have successfully mitigated risks related to cruise ships and their facilities.

CBP's Collection of Additional Passenger Data Could Enhance Cruise Ship Security

Although CBP currently uses manifest data provided by the cruise lines as part of the screening process for cruise ship passengers and crew, CBP officials stated the agency's experience in the aviation context suggests that the routine collection and analysis of additional passenger data could enhance the agency's cruise passenger screening process. However, CBP

is lacking full information on the benefit and cost of obtaining these data. Part of CBP's mission is to prevent terrorists and terrorist weapons from entering the United States, while also facilitating the flow of legitimate trade and travel. Under the Aviation and Transportation Security Act, air carriers operating flights in foreign air transportation to the United States are required to make Passenger Name Record information available to CBP⁴⁶ and under the agency's implementing regulations, CBP receives Passenger Name Record data in addition to manifest data for all passengers on international flights to or from the United States for purposes of ensuring aviation safety and protecting national security. Passengers provide data included in their Passenger Name Record to the airlines through the reservation process. Passenger Name Record data may include, among other things, a passenger's full itinerary, reservation booking date, phone number, and billing information, which is not usually available in the manifest data. According to CBP officials familiar with the process, Passenger Name Record data for airline passengers has been valuable because the additional information has helped the agency to better target passengers for inspection.⁴⁷ Specifically, the agency's National Targeting Center officials reported that airline Passenger Name Record data has allowed CBP to identify high risk passengers, including those who were not listed on watchlists—recognized by CBP as “previously unknown persons”—by (1) identifying links between passengers traveling with other high risk passengers or (2) identifying patterns of suspicious activity that have been identified with high risk passengers in the past. CBP provided examples of past efforts supporting the agency's view that the targeting of passengers for inspection through the use of Passenger Name Record data led to CBP taking adverse or enforcement actions, such as not allowing a high-risk passenger to board a flight. The examples indicate that CBP's targeting process identified passengers who represented various concerns, including terrorist-related concerns, as well as drug and immigration concerns. According to CBP, this process involved the use of Passenger Name Record data or the combination of this data with manifest data or other intelligence.⁴⁸ CBP officials also reported that Passenger Name Record data is provided to

⁴⁶Section 115 of Pub. L. No. 107-71, 115 Stat. 597 (2001) (codified at 49 U.S.C. 44909(c)(3)).

⁴⁷In November 2006, GAO issued a restricted report that discusses Passenger Name Record data. In May 2007, a public version of the report was issued. GAO, *Aviation Security: Efforts to Strengthen International Passenger Prescreening are Under Way, but Planning and Implementation Issues Remain*, [GAO-07-346](#) (Washington, D.C., May 16, 2007).

⁴⁸Detailed information regarding these cases is security sensitive information.

CBP earlier than manifest data, providing the agency with additional time to complete its passenger targeting process.⁴⁹

CBP program officials reported that having access to Passenger Name Record data for cruise line passengers could offer benefits similar to those derived from screening airline passengers, although CBP has not conducted a study or evaluation measuring the benefits, or determining the potential cost to the agency, cruise lines, and cruise line passengers. Our previous work identified evaluations as a way for agencies to explore the benefits of a program.⁵⁰ In addition, CBP's 2005-2010 Strategic Plan states that the agency should seek to improve the identification and targeting of potential terrorists and terrorist weapons, through risk management and automated advanced and enhanced information. Furthermore, a January 2010 Presidential memorandum states that DHS should aggressively pursue enhanced screening technology, protocols, and procedures, especially in regard to aviation and other transportation sectors, consistent with privacy rights and civil liberties.⁵¹ CBP does not require this information from all cruise lines on a systematic basis, although CBP reported that some CBP field units have access to some cruise lines' reservation systems and have received Passenger Name Record data on a case-by-case basis to enhance the information they have on passengers already identified for screening using other means. However, since field units do not have the same analytical tools as the National Targeting Center, they are less able to fully utilize the Passenger Name Record data on a systematic basis. CBP program officials stated that

⁴⁹CBP officials stated that there is always a concern about the accuracy and reliability of Passenger Name Record data for several reasons. First, this information is not standardized, that is, CBP receives Passenger Name Record data from 130 air carriers in about 100 different formats. CBP considers Passenger Name Record data as "dirty data" that requires great effort to process. Further, these data are collected or entered by the passenger or travel agent and there is the chance the data could be mistyped or a nickname could be used instead of a full name. CBP created algorithms in their system to account for similar names or acceptable misspellings to enhance the utility of the Passenger Name Record data.

⁵⁰GAO, *Program Evaluation: Studies Helped Agencies Measure or Explain Program Performance*, GAO/GGD-00-204 (Washington, D.C., September 29, 2000).

⁵¹This memorandum was issued after receiving the conclusions of two reviews related to the attempt to bring down a Detroit-bound flight on December 25, 2009, by detonating an explosive device. The first was a White House-led review of the U.S. terrorist watch list system and the performance of the intelligence, homeland security, and law enforcement communities related to the attempted attack. The second review was led by DHS on technology and procedures used for airport screening.

if the agency were to begin receiving and reviewing cruise line Passenger Name Record data, the effort would be highly automated and could allow for more effective and efficient targeting since the agency would receive the data earlier. Officials from CBP's Office of Information and Technology, however, stated that without specific requirements and further knowledge about the cruise lines' connectivity capabilities it is difficult to estimate the cost to both CBP and the cruise lines of implementing the technological aspects of a requirement to obtain Passenger Name Record data from the cruise lines. Based on CBP's experience with implementing such a requirement for the air carriers, CBP's Office of Information and Technology officials stated that there were costs to CBP and the air carriers for infrastructure, licensing, and ongoing maintenance; however, the cost depended on the air carrier's existing system and infrastructure at the time the requirement was being implemented. As of January 2010, CBP was spending about \$3 million per year to maintain connections with most of the air carriers, and officials stated that creating and maintaining connections with cruise line reservation systems would require new infrastructure and costs.

According to a representative from the Cruise Lines International Association, the cruise lines would be willing to systematically share all Passenger Name Record data with CBP if required to do so. However, the Cruise Lines International Association did not know if this type of requirement would deter passengers from booking cruises. One cruise line official we interviewed stated that such a requirement would not be a major burden for their cruise line to implement, while another cruise line official stated that such a requirement could have significant cost implications for their cruise line depending on what data would be required and what requirements would be established for transmitting it to CBP, among other things.

In addition to assessing the impact that such a data requirement would have on agency and industry resources, other aspects of such a requirement, such as verifying the agency's statutory authority and assessing the impact on privacy issues, would also be important to study. Although CBP program officials stated that the agency's regulations for collecting Passenger Name Record data apply to passengers traveling on international flights and not passengers on cruise ships, CBP officials, including a representative from CBP's Chief Counsel, reported that various statutory authorities collectively provide the agency with the authority to require such information from the cruise lines. In addition, similar to the Passenger Name Record data requirement for air carriers, other important considerations for determining the cost and benefit of such a requirement

for the cruise lines would be (1) assessing the privacy impacts of such a requirement on cruise passengers and developing any necessary public disclosure documents, and (2) determining the appropriate agreements that may be needed with other countries regarding the sharing and collection of this data. The Privacy Act of 1974⁵² and the E-Government Act of 2002,⁵³ in general, require federal agencies to protect personal privacy by, among other ways, limiting the disclosure of personal information and informing the public about how personal data are being used and protected. The E-Government Act and implementing Office of Management and Budget guidance⁵⁴ require that agencies analyze how information is handled to (1) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (2) determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.⁵⁵ Another privacy consideration would be the availability of a redress mechanism for individuals who felt that they had been unfairly denied boarding as a result of the screening process. As reported in DHS's 2006 report on Privacy and Civil Liberties, a robust redress program is essential for any federal program that uses personal information in order to grant or deny to individuals a right, privilege, or benefit.⁵⁶ DHS's Traveler Redress Inquiry Program serves as a single point of contact for individuals who have inquiries or seek resolution regarding difficulties they experienced during

⁵²Pub. L. No. 93-579, 88 Stat. 1879 (1974).

⁵³Pub. L. No. 107-347, 116 Stat. 2899 (2002).

⁵⁴Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22 (Washington, D.C.: Sept. 26, 2003).

⁵⁵The Privacy Act places limitations on agencies' collection, use, and disclosure of personal information maintained in systems of records, which are groups of personal information that are maintained by an agency from which personal information is retrieved by an individual's name or identifier. Among the act's provisions are requirements for agencies to give notice to the public about the use of their personal information. Also, when agencies establish or make changes to a system of records, they must notify the public by a notice in the *Federal Register* about the type of data collected; the types of individuals about whom information is collected; the intended "routine" uses of the data; the policies and practices regarding data storage, retrievability, access controls, retention, and disposal; and procedures that individuals can use to review and correct personal information. The E-Government Act of 2002 requires agencies to conduct a privacy impact assessment when using information technology to process personal information.

⁵⁶DHS, *Report on Effects on Privacy and Civil Liberties* (April 27, 2006).

their travel screening at transportation hubs—like airports and train stations—or crossing U.S. borders. With respect to the collection of Passenger Name Record data from other countries, the privacy laws of other countries must also be considered. For example, in 2002, when air carriers operating international flights to and from the United States were first required to submit Passenger Name Record data to CBP, concerns about privacy were raised, and a permanent agreement on the sharing of this data between the United States and the European Union took several years to finalize. Without obtaining full information on the benefit and cost of requiring cruise lines to submit Passenger Name Record data to CBP and considering the associated privacy implications, CBP is not in the best position to determine whether the benefits of such a requirement would outweigh the potential costs to the agency and industry, and the risks to passenger privacy.

Conclusions

Given the number of passengers that travel on cruise ships each year and the attractiveness of these vessels as terrorist targets, it is important that the risk to cruise ships is assessed and actions are taken to help ensure the security of these ships and their facilities. Federal agencies and maritime security stakeholders, including cruise lines, have implemented various measures to better secure cruise ships and their facilities. As examples, the Coast Guard provides escorts for cruise ships to prevent waterside attacks and CBP screens passengers using manifest data to prevent terrorists from boarding cruise ships. Although these measures have been implemented and there has been no recent credible terrorist threat against cruise ships, this does not preclude the possibility of such an incident occurring in the future, particularly given the existence of terrorist groups that have the capability to attack a cruise ship. Moreover, the President's 2010 memorandum directing DHS to aggressively pursue enhanced screening efforts further underscores the potential importance of this type of security action. By conducting a study to determine whether requiring cruise lines to provide automated Passenger Name Record data on a systematic basis is cost effective and addresses privacy implications, CBP would be in a better position to determine whether additional actions should be taken to augment security through enhanced screening of cruise ship passengers.

Recommendation for Executive Action

To enhance the existing screening process for cruise ship passengers, we recommend that the CBP Commissioner conduct a study to determine whether requiring cruise lines to provide automated Passenger Name Record data to CBP on a systematic basis would benefit homeland

security, and if found to be of substantial benefit, determine the appropriate mechanism through which to issue this requirement. The scope of the study should include potential benefits to security, any need for additional authority and international agreements, resource implications for CBP and the cruise industry, privacy concerns, and any implementation issues related to the automated transfer of Passenger Name Record data from the cruise lines to CBP.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Homeland Security, State, and Defense for their review and comment. The Department of State responded that they did not have any comments on the report. We requested comments from the Department of Defense, but none were provided. The Department of Homeland Security, in its written comments, concurred with our findings and recommendation.

Regarding our recommendation, DHS responded that CBP will conduct a study that outlines the security, cost, and facilitation benefits an automated Passenger Name Record system would bring to homeland security and the cruise line industry. Upon completion of the study, CBP will determine if the benefits of such a program are substantial enough to pursue full implementation of the program. DHS officials also provided technical comments on the draft that have been incorporated, as appropriate. Written comments from DHS are reproduced in appendix I.

As arranged with your office we plan no further distribution until 30 days after the date of this report. At that time, we will send copies of this report to the Secretaries of Homeland Security, State, and Defense, and other interested parties. In addition, the report will be available on GAO's Web site at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix II.

Sincerely yours,

A handwritten signature in black ink, appearing to read "Stephen Caldwell". The signature is fluid and cursive, with a checkmark-like flourish at the end.

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Appendix I: Agency Comments



Homeland
Security

March 18, 2010

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

Dear Mr Caldwell:

The Department of Homeland Security (DHS) appreciates the opportunity to review and comment on the Government Accountability Office (GAO) report, GAO-10-400: *"Maritime Security: Varied Actions Taken to Enhance Cruise Ship Security, but Some Vulnerabilities Remain"*. DHS generally concurs with the report's findings and recommendation. We have provided our recommendation-specific comments below; technical comments have been provided under separate cover.

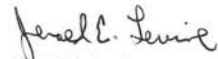
Recommendation #1: To enhance the existing screening process for cruise ship passengers, we recommend that the U.S. Customs and Border Protection (CBP) Commissioner conduct a study to determine whether requiring cruise lines to provide automated Passenger Name Record (PNR) data to CBP on a systematic basis would benefit homeland security, and if found to be of substantial benefit, determine the appropriate mechanism through which to issue this requirement. The scope of the study should include potential benefits to security, any need for additional authority and international agreements, resource implications for CBP and the cruise industry, privacy concerns, and any implementation issues related to the automated transfer of PNR data from the cruise lines to CBP.

Response: CBP currently receives PNR data from the airline industry, which has proven invaluable in identifying persons of interest, well in advance of their intended travel. To determine whether requiring PNR data would yield the same benefits in the commercial cruise environment, CBP will conduct a study that outlines the security, cost, and facilitation benefits an automated PNR system would bring to homeland security and the cruise line industry. Upon completion of the study, CBP will determine if the benefits of such a program are substantial enough to pursue full implementation of the program.

- 2 -

Again, we appreciate the opportunity to review and comment on this draft report and we look forward to working with you on future homeland security issues.

Sincerely,



Jerald E. Levine
Director
Departmental GAO/OIG Liaison Office

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, Dawn Hoff, Assistant Director, and Jonathan Bachman, analyst-in-charge, managed this assignment. Tracey Cross made significant contributions to the work. Stanley Kostyla assisted with design and methodology. Geoffrey Hamilton provided legal support. Linda Miller provided assistance in report preparation. Josh Ormond developed the report's graphic.

Related GAO Products

Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers. [GAO-10-12](#). Washington, D.C.: October 30, 2009.

Maritime Security: Vessel Tracking Systems Provide Key Information, but the Need for Duplicate Data Should be Reviewed. [GAO-09-337](#). Washington, D.C.: March 17, 2009.

Supply Chain Security: CBP Works with International Entities to Promote Global Customs Security Standards and Initiatives, but Challenges Remain. [GAO-08-538](#). Washington, D.C.: August 15, 2008.

Maritime Security: National Strategy and Supporting Plans Were Generally Well-Developed and Are Being Implemented. [GAO-08-672](#). Washington, D.C.: June 20, 2008.

Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers. [GAO-08-533T](#). Washington, D.C.: June 12, 2008.

Supply Chain Security: U.S. Customs and Border Protection Has Enhanced Its Partnership with Import Trade Sectors, but Challenges Remain in Verifying Security Practices. [GAO-08-240](#). Washington, D.C.: April 25, 2008.

Maritime Security: Coast Guard Inspections Identify and Correct Facility Deficiencies, but More Analysis Needed of Program's Staffing, Practices, and Data. [GAO-08-12](#). Washington, D.C.: February 14, 2008.

Supply Chain Security: Examination of High-Risk Cargo at Foreign Seaports Have Increased, but Improved Data Collection and Performance Measures Are Needed. [GAO-08-187](#). Washington, D.C.: January 25, 2008.

Maritime Security: Federal Efforts Needed to Address Challenges in Preventing and Responding to Terrorist Attacks on Energy Commodity Tankers. [GAO-08-141](#). Washington, D.C.: December 10, 2007.

Maritime Security: The SAFE Port Act: Status and Implementation One Year Later. [GAO-08-126T](#). Washington, D.C.: October 30, 2007.

Combating Nuclear Smuggling: Additional Actions Needed to Ensure Adequate Testing of Next Generation Radiation Detection Equipment. [GAO-07-1247T](#). Washington, D.C.: September 18, 2007.

Information on Port Security in the Caribbean Basin. [GAO-07-804R](#). Washington, D.C.: June 29, 2007.

Port Risk Management: Additional Federal Guidance Would Aid Ports in Disaster Planning and Recovery. [GAO-07-412](#). Washington, D.C.: March 28, 2007.

Maritime Security: Public Safety Consequences of a Terrorist Attack on a Tanker Carrying Liquefied Natural Gas Need Clarification. [GAO-07-316](#). Washington, D.C.: February 22, 2007.

Coast Guard: Observations on the Preparation, Response, and Recovery Missions Related to Hurricane Katrina. [GAO-06-903](#). Washington, D.C.: July 31, 2006.

Maritime Security: Information Sharing Efforts Are Improving. [GAO-06-933T](#). Washington, D.C.: July 10, 2006.

Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System. [GAO-06-591T](#). Washington, D.C.: March 30, 2006.

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. [GAO-06-91](#). Washington, D.C.: December 15, 2005.

Homeland Security: Key Cargo Security Programs Can Be Improved. [GAO-05-466T](#). Washington, D.C.: May 26, 2005.

Maritime Security: Enhancements Made, But Implementation and Sustainability Remain Key Challenges. [GAO-05-448T](#). Washington, D.C.: May 17, 2005.

Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts. [GAO-05-557](#). Washington, D.C.: April 26, 2005.

Maritime Security: New Structures Have Improved Information Sharing, but Security Clearance Processing Requires Further Attention. [GAO-05-394](#). Washington, D.C.: April 15, 2005.

Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security. [GAO-05-404](#). Washington, D.C.: March 11, 2005.

Maritime Security: Better Planning Needed to Help Ensure an Effective Port Security Assessment Program. [GAO-04-1062](#). Washington, D.C.: September 30, 2004.

Maritime Security: Partnering Could Reduce Federal Costs and Facilitate Implementation of Automatic Vessel Identification System. [GAO-04-868](#). Washington, D.C.: July 23, 2004.

Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security. [GAO-04-838](#). Washington, D.C.: June 30, 2004.

Homeland Security: Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection. [GAO-04-557T](#). Washington, D.C.: March 31, 2004.

Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers. [GAO-04-325T](#). Washington, D.C.: December 16, 2003.

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

Combating Terrorism: Interagency Framework and Agency Programs to Address the Overseas Threat. [GAO-03-165](#). Washington, D.C.: May 23, 2003.

Nuclear Nonproliferation: U.S. Efforts to Combat Nuclear Smuggling. [GAO-02-989T](#). Washington, D.C.: July 30, 2002.

Coast Guard: Vessel Identification System Development Needs to Be Reassessed. [GAO-02-477](#). Washington, D.C.: May 24, 2002.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

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

Congressional Relations

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

Public Affairs

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

