



Report to the Chairman, Committee on
Commerce, Science, and
Transportation, U.S. Senate

June 2014

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Better Address Port Cybersecurity

GAO Highlights

Highlights of [GAO-14-459](#), a report to the Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate

Why GAO Did This Study

U.S. maritime ports handle more than \$1.3 trillion in cargo annually. The operations of these ports are supported by information and communication systems, which are susceptible to cyber-related threats. Failures in these systems could degrade or interrupt operations at ports, including the flow of commerce. Federal agencies—in particular DHS—and industry stakeholders have specific roles in protecting maritime facilities and ports from physical and cyber threats.

GAO's objective was to identify the extent to which DHS and other stakeholders have taken steps to address cybersecurity in the maritime port environment. GAO examined relevant laws and regulations; analyzed federal cybersecurity-related policies and plans; observed operations at three U.S. ports selected based on being a high-risk port and a leader in calls by vessel type, e.g. container; and interviewed federal and nonfederal officials.

What GAO Recommends

GAO recommends that DHS direct the Coast Guard to (1) assess cyber-related risks, (2) use this assessment to inform maritime security guidance, and (3) determine whether the sector coordinating council should be reestablished. DHS should also direct FEMA to (1) develop procedures to consult DHS cybersecurity experts for assistance in reviewing grant proposals and (2) use the results of the cyber-risk assessment to inform its grant guidance. DHS concurred with GAO's recommendations.

View [GAO-14-459](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov.

June 2014

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Better Address Port Cybersecurity

What GAO Found

Actions taken by the Department of Homeland Security (DHS) and two of its component agencies, the U.S. Coast Guard and Federal Emergency Management Agency (FEMA), as well as other federal agencies, to address cybersecurity in the maritime port environment have been limited.

- While the Coast Guard initiated a number of activities and coordinating strategies to improve physical security in specific ports, it has not conducted a risk assessment that fully addresses cyber-related threats, vulnerabilities, and consequences. Coast Guard officials stated that they intend to conduct such an assessment in the future, but did not provide details to show how it would address cybersecurity. Until the Coast Guard completes a thorough assessment of cyber risks in the maritime environment, the ability of stakeholders to appropriately plan and allocate resources to protect ports and other maritime facilities will be limited.
- Maritime security plans required by law and regulation generally did not identify or address potential cyber-related threats or vulnerabilities. This was because the guidance issued by Coast Guard for developing these plans did not require cyber elements to be addressed. Officials stated that guidance for the next set of updated plans, due for update in 2014, will include cybersecurity requirements. However, in the absence of a comprehensive risk assessment, the revised guidance may not adequately address cyber-related risks to the maritime environment.
- The degree to which information-sharing mechanisms (e.g., councils) were active and shared cybersecurity-related information varied. Specifically, the Coast Guard established a government coordinating council to share information among government entities, but it is unclear to what extent this body has shared information related to cybersecurity. In addition, a sector coordinating council for sharing information among nonfederal stakeholders is no longer active, and the Coast Guard has not convinced stakeholders to reestablish it. Until the Coast Guard improves these mechanisms, maritime stakeholders in different locations are at greater risk of not being aware of, and thus not mitigating, cyber-based threats.
- Under a program to provide security-related grants to ports, FEMA identified enhancing cybersecurity capabilities as a funding priority for the first time in fiscal year 2013 and has provided guidance for cybersecurity-related proposals. However, the agency has not consulted cybersecurity-related subject matter experts to inform the multi-level review of cyber-related proposals—partly because FEMA has downsized the expert panel that reviews grants. Also, because the Coast Guard has not assessed cyber-related risks in the maritime risk assessment, grant applicants and FEMA have not been able to use this information to inform funding proposals and decisions. As a result, FEMA is limited in its ability to ensure that the program is effectively addressing cyber-related risks in the maritime environment.

Contents

Letter		1
	Background	4
	Federal Stakeholders Have Taken Limited Actions to Address Cybersecurity in the Maritime Port Environment	16
	Conclusions	28
	Recommendations for Executive Action	28
	Agency Comments and Our Evaluation	29
Appendix I	Objective, Scope, and Methodology	32
Appendix II	Additional Federal Maritime Cybersecurity Actions	36
Appendix III	Full Text for Figure 1 on Examples of Technologies Used in Maritime Port Environments	43
Appendix IV	Comments from the Department of Homeland Security	44
Appendix V	GAO Contacts and Staff Acknowledgments	47
Related GAO Products		48
Tables		
	Table 1: Sources of Cyber-based Threats	7
	Table 2: Types of Exploits	8
Figures		
	Figure 1: Examples of Technologies Used in Maritime Port Environments	6

Abbreviations

CBP	U.S. Customs and Border Protection
Coast Guard	U.S. Coast Guard
DHS	Department of Homeland Security
FEMA	Federal Emergency Management Agency
HSPD-7	Homeland Security Presidential Directive 7
ISAC	information sharing and analysis center
IT	information technology
MTSA	Maritime Transportation Security Act of 2002
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
PPD-21	Presidential Policy Directive 21
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.



June 5, 2014

The Honorable John D. Rockefeller IV
Chairman
Committee on Commerce, Science,
and Transportation
United States Senate

Dear Mr. Chairman:

An essential element of the nation's transportation critical infrastructure,¹ U.S. maritime ports are part of an economic engine handling more than \$1.3 trillion in cargo annually. A major disruption in the maritime transportation system could have a widespread impact on global shipping, international trade, and the global economy. The potential economic impact caused by a disruption in port operations underscores the importance of ensuring that ports remain operational to the maximum extent possible.

Information and communication systems support the operation of these ports, and failures in these systems as a result of unintended or malicious incidents could degrade or interrupt port operations and the flow of cargo or, as a recently reported incident showed, allow criminal activity to occur unimpeded. Since 2003, we have identified the protection of systems supporting our nation's critical infrastructure as a government-wide high-

¹The term "critical infrastructure" as defined in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) refers to systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. 42 U.S.C. § 5195c(e). The transportation systems sector (which includes the maritime mode as a subsector) is 1 of 16 critical infrastructure sectors established by federal policy. The other sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; and water and wastewater systems.

risk area, and we continued to do so in the most recent update to our high-risk list.²

In addition, we recently testified that the federal government needs to address pressing challenges to its cybersecurity and accelerate progress in bolstering the cybersecurity posture of the nation.³ As computer technology has advanced, our nation's critical infrastructures, such as power distribution, water supply, telecommunications, and emergency services, have become increasingly dependent on computerized information systems and electronic data to carry out operations and to process, maintain, and report essential information. The security of these systems and data is essential to protecting national security, economic prosperity, and public health and safety. As we have reported, (1) cyber threats to critical infrastructure are evolving and growing, (2) cyber incidents affecting computer systems and networks continue to rise, and (3) the federal government continues to face challenges in a number of key aspects of its approach to protecting the nation's critical infrastructure.⁴

A combination of federal, state, and local governments; port authorities; and private companies own and operate U.S. ports and maritime facilities and are ultimately responsible for protecting their assets from physical and cyber-related threats. Federal law and policy establish a role for federal agencies, in particular, the Department of Homeland Security (DHS), in protecting maritime facilities and ports from physical and cyber-related threats.

²GAO's biennial High-Risk List identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need to address challenges to economy, efficiency, or effectiveness. We have designated federal information security as a high-risk area since 1997; in 2003, we expanded this high risk area to include protecting systems supporting our nation's critical infrastructure. See GAO, *High-Risk Series: An Update*, [GAO-13-283](#) (Washington, D.C.: February 2013).

³GAO, *Government Efficiency and Effectiveness: Views on the Progress and Plans for Addressing Government-wide Management Challenges*, [GAO-14-436T](#) (Washington, D.C.: Mar. 12, 2014).

⁴GAO, *Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented*, [GAO-13-187](#) (Washington, D.C.: Feb. 14, 2013).

At your request, we reviewed cybersecurity-related threats and actions taken by stakeholders in the maritime environment. Our specific objective was to identify the extent to which DHS and other stakeholders have taken steps to address cybersecurity⁵ in the maritime port environment.

To conduct our evaluation, we analyzed relevant maritime laws and regulations for cybersecurity-related authorities, and analyzed cybersecurity-related federal policies and plans. Based on these analyses, we identified relevant federal entities, including the Departments of Homeland Security (including the U.S. Coast Guard (Coast Guard) and Federal Emergency Management Agency (FEMA)), Commerce, Defense, Justice, and Transportation. We also identified activities that federal and nonfederal maritime stakeholders should be performing to mitigate cyber threats to their operations. We focused on the information and communications technology used to operate port facilities. We did not include aspects of the maritime environment such as vessels, off-shore platforms, inland waterways, intermodal connections,⁶ and federally managed information and communication technology. We visited a non-projectable sample of three domestic ports to identify the types of technologies used during port operations and to examine port area and facility security plans. These ports were selected based on their identification as both high-risk ports and as national leaders in calls by specific types of vessels—oil and natural gas, containers, and dry bulk. We also gathered and analyzed evidence of stakeholder actions taken to address cybersecurity issues as reflected in security plans, and interviewed federal and nonfederal officials who have roles in protecting maritime facilities and ports from physical or cyber-related threats.

We conducted this performance audit from April 2013 to June 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

⁵“Cybersecurity” means the ability to protect or defend the use of cyberspace from cyber attacks. “Cyberspace” is defined as a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. A “cyber attack” is further defined as an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure, or destroying the integrity of the data or stealing controlled information.

⁶Intermodal connections link the various transportation modes, e.g., maritime ports and related facilities, highways, rail, and air.

sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Appendix I discusses our objective, scope, and methodology in greater detail.

Background

The United States has approximately 360 commercial sea and river ports that handle more than \$1.3 trillion in cargo annually. A wide variety of goods, including automobiles, grain, and millions of cargo containers, travel through these ports each day. While no two ports are exactly alike, many share certain characteristics, like their size, general proximity to a metropolitan area, the volume of cargo being processed, and connections to complex transportation networks designed to move cargo and commerce as quickly as possible, that make them vulnerable to physical security threats.

Entities within the maritime port environment are also vulnerable to cyber-based threats because maritime stakeholders rely on numerous types of information and communications technologies to manage the movement of cargo throughout ports. Examples of these technologies include the following:

- **Terminal operating systems:** These are information systems used by terminal operators to, among other things, control container movements and storage. For example, the terminal operating system is to support the logistical management of containers while in the terminal operator's possession, including container movement and storage. To enhance the terminal operator's operations, the system can also be integrated with other systems and technologies, such as financial systems, mobile computing, optical character recognition, and radio frequency identification systems.
- **Industrial control systems:** In maritime terminals, industrial control systems⁷ facilitate the movement of goods throughout the terminal using conveyor belts or pipelines to various structures (e.g., refineries, processing plants, and storage tanks).

⁷Industrial control systems are automated systems used to control industrial processes such as manufacturing, product handling, production, and distribution. According to maritime sector documentation, control systems are used to operate motors, pumps, valves, signals, lighting, and access controls.

-
- **Business operations systems:** These are information and communications technologies used to help support the business operations of the terminal, such as communicating with customers and preparing invoices and billing documentation. These systems can include e-mail and file servers, enterprise resource planning systems,⁸ networking equipment, phones, and fax machines.
 - **Access control and monitoring systems:** Information and communication technology can also be used to support physical security operations at a port. For example, camera surveillance systems can be connected to information system networks to facilitate remote monitoring of port facilities, and electronically enabled physical access control devices can be used to protect sensitive areas of a port.

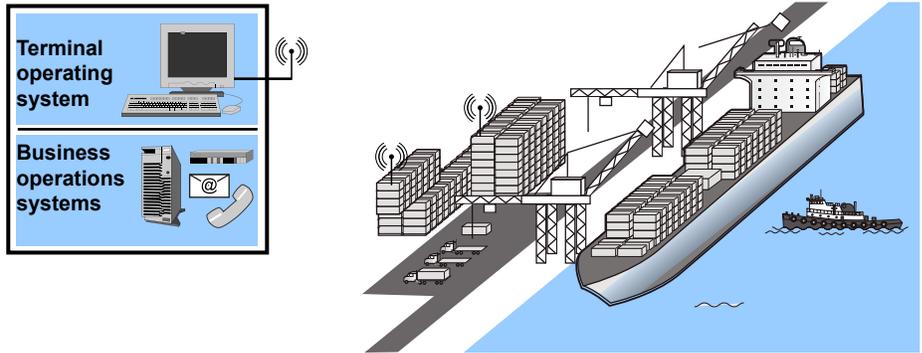
See figure 1, an interactive graphic, for an overview of the technologies used in the maritime port environment. See appendix III for a printable version.

⁸An enterprise resource planning system is an automated system using commercial off-the-shelf software consisting of multiple, integrated functional modules that perform a variety of business-related tasks such as general ledger accounting, payroll, and supply chain management.

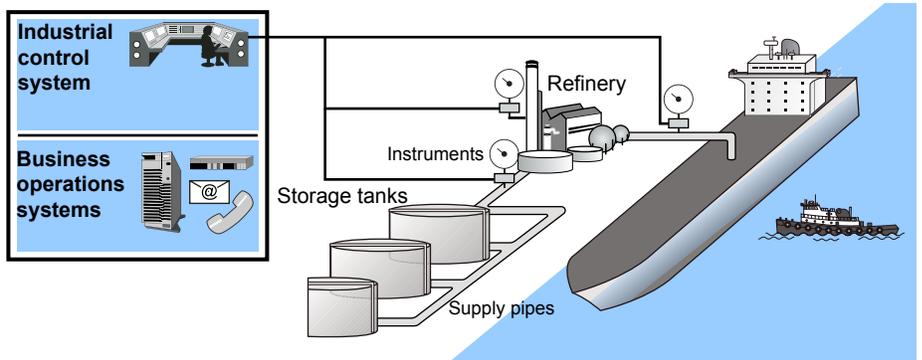
Interactive graphic Figure 1: Examples of Technologies Used in Maritime Port Environments

Move mouse over blue system names to get descriptions of the systems. See appendix III for noninteractive version of this graphic.

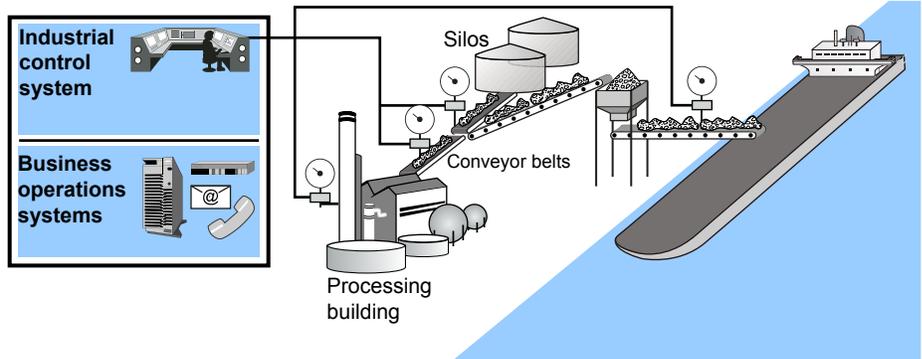
Container



Bulk liquid



Dry bulk



Source: GAO analysis of maritime sector information; Art Explosion (clip art).

The location of the entity that manages these systems can also vary. Port facility officials we interviewed stated that some information technology systems used by their facilities are managed locally at the ports, while others are managed remotely from locations within and outside the United States.

In addition, other types of automated infrastructure are used in the global maritime trade industry. For example, some ports in Europe use automated ground vehicles and stacking cranes to facilitate the movement of cargo throughout the ports.

The Nation and Its Ports Face an Evolving Array of Cyber-Based Threats

Like threats affecting other critical infrastructures, threats to the maritime information technology (IT) infrastructure can come from a wide array of sources. For example, advanced persistent threats—where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives—pose increasing risk. Threat sources include corrupt employees, criminal groups, hackers, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary or political gain or mischief, among other things. Table 1 describes the sources of cyber-based threats in more detail.

Table 1: Sources of Cyber-based Threats

Threat source	Description
Bot-network operators	Bot-net operators use a network of compromised, remotely controlled systems, referred to as a bot-net, to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or services to relay spam or phishing attacks).
Business competitors	Companies that compete against or do business with a target company may seek to obtain sensitive information to improve their competitive advantage in various areas, such as pricing, manufacturing, product development, and contracting.
Criminal groups	Organized criminal groups use spam, phishing, and spyware/malware to commit identity theft, online fraud, and computer extortion.
Hackers	Hackers break into networks for the thrill of the challenge, bragging rights in the hacker community, revenge, stalking, monetary gain, and political activism, among other reasons. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use.

Threat source	Description
Insiders	A disgruntled or corrupt organization insider is a source of computer crime. The insider may not need a great deal of knowledge about computer intrusions because his or her knowledge of a target system is sufficient to allow unrestricted access to cause damage to the system or to steal system data. The insider threat includes malicious current and former employees and contractors hired by the organization, as well as careless or poorly trained employees who may inadvertently introduce malware into systems.
Nations	Nations use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of citizens across the country. In his January 2012 testimony, the Director of National Intelligence stated that, among state actors, China and Russia are of particular concern.
Phishers	Individuals or small groups execute phishing schemes in an attempt to steal identities or information for monetary gain. A phisher may also use spam and spyware or malware to accomplish their objectives.
Spammers	An individual or organization that distributes unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware or malware, or attack organizations (e.g., a denial of service).
Spyware or malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware.
Terrorists	A terrorist seeks to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the economy, and damage public morale and confidence. The terrorist may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

Source: GAO analysis based on data from the Director of National Intelligence, Department of Justice, Central Intelligence Agency, National Institute of Standards and Technology, and Software Engineering Institute's CERT® Coordination Center.

These sources of cyber threats may make use of various cyber techniques, or exploits, to adversely affect information and communications networks. Types of exploits include denial-of-service attacks, phishing, Trojan horses, viruses, worms, and attacks on the IT supply chains that support the communications networks. Table 2 describes the types of exploits in more detail.

Table 2: Types of Exploits

Type of exploit	Description
Denial of service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed denial of service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Phishing	A digital form of social engineering that uses authentic-looking, but fake, e-mails to request information from users or direct them to a fake website that requests information.
Trojan Horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a useful program that a user would likely execute.

Type of exploit	Description
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user. A virus might corrupt or delete data on a computer, use an e-mail program to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Worm	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread. Unlike a computer virus, a worm does not require human involvement to propagate.
Exploits affecting the information technology supply chain	The installation of hardware or software that contains malicious logic (like a logic bomb, Trojan horse, or a virus) or an unintentional vulnerability (the result of an existing defect, such as a coding error) or that may be counterfeited. A supply chain threat can also come from a failure or disruption in the production of a critical product, or a reliance on a malicious or unqualified service provider for the performance of technical services.

Source: GAO analysis of unclassified government and nongovernment data.

Similar to those in the United States, ports elsewhere in the world also rely on information and communications technology to facilitate their operations, and concerns about the potential impact of cybersecurity threats and vulnerabilities on these operations have been raised. For example, according to a 2011 report issued by the European Network and Information Security Agency,⁹ the maritime environment, like other sectors, increasingly relies on information and communications systems to optimize its operations, and the increased dependency on these systems, combined with the operational complexity and multiple stakeholders involved, make the environment vulnerable to cyber attacks. In addition, Australia's Office of the Inspector of Transport Security reported in June 2012 that a cyber attack is probably the most serious threat to the integrity of offshore oil and gas facilities and land-based production.¹⁰

In addition, a recently reported incident highlights the risk that cybersecurity threats pose to the maritime port environment. Specifically, according to Europol's European Cybercrime Center, a cyber incident was reported in 2013 (and corroborated by the Federal Bureau of Investigation) in which malware was installed on a computer at a foreign port.¹¹ The reported goal of the attack was to track the movement of

⁹European Network and Information Security Agency, *Analysis of Cyber Security Aspects in the Maritime Sector* (Heraklion, Greece: November 2011).

¹⁰*Offshore Oil and Gas Resources Sector Security Inquiry* © Commonwealth of Australia (2012).

¹¹Europol European Cybercrime Center, *Cyber Bits: Hackers deployed to facilitate drugs smuggling* (The Hague, Netherlands: June 2013).

shipping containers for smuggling purposes. A criminal group used hackers to break into the terminal operating system to gain access to security and location information that was leveraged to remove the containers from the port.

Federal Plans and Policies Establish Responsibilities for Securing Cyber-Reliant Critical Infrastructure

Port owners and operators are responsible for the cybersecurity of their operations, and federal plans and policies specify roles and responsibilities for federal agencies to support those efforts. In particular, the National Infrastructure Protection Plan (NIPP), a planning document originally developed pursuant to the Homeland Security Act of 2002 and Homeland Security Presidential Directive 7 (HSPD-7),¹² sets forth a risk management framework to address the risks posed by cyber, human, and physical elements of critical infrastructure. It details the roles and responsibilities of DHS in protecting the nation's critical infrastructures; identifies agencies that have lead responsibility for coordinating with the sectors (referred to as sector-specific agencies); and specifies how other federal, state, regional, local, tribal, territorial, and private-sector stakeholders should use risk management principles to prioritize protection activities within and across sectors.¹³

In addition, NIPP sets up a framework for operating and sharing information across and between federal and nonfederal stakeholders within each sector that includes the establishment of two types of councils: sector coordinating councils and government coordinating

¹²See 6 U.S.C. § 121(d)(5); the White House, Homeland Security Presidential Directive 7 (Washington, D.C.: December 2003). Presidential Policy Directive 21 (PPD-21) revoked HSPD-7, but plans developed pursuant to HSPD-7 remain in effect until specifically revoked or superseded. PPD-21 also required DHS to provide to the President a successor to the National Infrastructure Protection Plan, which DHS released in December 2013. See DHS, *National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

¹³NIPP was first issued in June 2006. It was updated in 2009 and again in December 2013, in part, to reflect changes in federal cybersecurity policy since 2009. It identifies the roles and responsibilities of DHS, sector-specific agencies, and private sector partners.

councils.¹⁴ The 2006 and 2009 NIPPs identified the U.S. Coast Guard as the sector-specific agency for the maritime mode of the transportation sector.¹⁵ In this role, the Coast Guard is to coordinate protective programs and resilience strategies for the maritime environment.

Under NIPP, each critical infrastructure sector is also to develop a sector-specific plan to detail the application of its risk management framework for the sector. The 2010 Transportation Systems Sector-Specific Plan includes an annex for the maritime mode of transportation.¹⁶ The maritime annex is considered an implementation plan that details the individual characteristics of the maritime mode and how it will apply risk management, including a formal assessment of risk, to protect its systems, assets, people, and goods.

In February 2013, the White House issued Presidential Policy Directive 21,¹⁷ which shifted the nation's focus from protecting critical infrastructure against terrorism toward protecting and securing critical infrastructure and increasing its resilience against all hazards, including natural disasters, terrorism, and cyber incidents. The directive identified sector-specific

¹⁴Sector coordinating councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum of key stakeholders within a sector; and serve as a principal entry point for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. Government coordinating councils are established to enable interagency and intergovernmental coordination, and include representatives across various levels of government (federal and state/local/tribal/territorial) as appropriate to the risk and operational landscape of each sector. Representatives from the Departments of Commerce, Defense, Homeland Security, Justice, and Transportation make up the Maritime Mode Government Coordinating Council.

¹⁵The 2013 NIPP designates DHS and the Department of Transportation as co-sector-specific agencies with responsibility for the maritime mode. Within DHS, Coast Guard has primary responsibility for the maritime mode.

¹⁶DHS, *Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan* (Washington, D.C.: 2010).

¹⁷PPD-21, issued on February 12, 2013, revoked HSPD-7. However, plans developed pursuant to HSPD-7 are to remain in effect until specifically revoked or superseded. PPD-21 re-aligned the HSPD-7 critical infrastructure sectors and reduced the number from 18 to 16. The 16 critical infrastructure sectors are chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

agency roles and responsibilities to include, among other things, serving as a day-to-day federal interface for the prioritization and coordination of sector-specific activities.

In December 2013, DHS released an updated version of NIPP. The 2013 NIPP reaffirms the role of various coordinating structures (such as sector coordinating councils and government coordinating councils) and integrates cyber and physical security and resilience efforts into an enterprise approach for risk management, among other things. The 2013 NIPP also reiterates the sector-specific agency roles and responsibilities as defined in Presidential Policy Directive 21.

In addition, in February 2013 the President signed Executive Order 13636 for improving critical infrastructure cybersecurity.¹⁸ The executive order states that, among other things

- the National Institute of Standards and Technology shall lead the development of a cybersecurity framework that will provide technology-neutral guidance;
- the policy of the federal government is to increase the volume, timeliness, and quality of cyber threat information sharing with the U.S. private sector;
- agencies with responsibility to regulate the security of critical infrastructure shall consider prioritized actions to promote cyber security; and
- DHS shall identify critical infrastructure where a cybersecurity incident could have a catastrophic effect on public health or safety, economic security, or national security.

Federal Laws and Implementing Regulations Establish Security Requirements for the Maritime Sector

The primary laws and regulations that establish DHS's maritime security requirements include the Maritime Transportation Security Act of 2002 (MTSA),¹⁹ the Security and Accountability for Every Port Act of 2006 (SAFE Port Act),²⁰ and Coast Guard's implementing regulations for these laws.

¹⁸Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 19, 2013).

¹⁹Pub. L. No. 107-295, 116 Stat. 2064.

²⁰Pub. L. No. 109-347, 120 Stat. 1884.

Enacted in November 2002, MTSA requires a wide range of security improvements for protecting our nation's ports, waterways, and coastal areas. DHS is the lead agency for implementing the act's provisions and relies on its component agencies, including the Coast Guard and FEMA, to help implement the act.²¹ The Coast Guard is responsible for security of U.S. maritime interests, including completion of security plans related to geographic areas around ports with input from port stakeholders. These plans are to assist the Coast Guard in the protection against transportation security incidents across the maritime port environment.²² The Coast Guard has designated a captain of the port within each of 43 geographically defined port areas²³ across the nation who is responsible for overseeing the development of the security plans within his or her respective geographic region.

The MTSA implementing regulations, developed by the Coast Guard, require the establishment of area maritime security committees across all port areas.²⁴ The committees for each of the 43 identified port areas, which are organized by the Coast Guard, consist of key stakeholders who (1) may be affected by security policies and (2) share information and develop port security plans. Members of the committees can include a diverse array of port stakeholders, including federal, state, local, tribal, and territorial law enforcement agencies, as well as private sector entities such as terminal operators, yacht clubs, shipyards, marine exchanges, commercial fishermen, trucking and railroad companies, organized labor, and trade associations. These committees are to identify critical port infrastructure and risks to the port, develop mitigation strategies for these risks, and communicate appropriate security information to port stakeholders.

²¹GAO, *Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act*, [GAO-12-1009T](#) (Washington, D.C.: Sept. 11, 2012).

²²A transportation security incident is defined as a security incident resulting in a significant loss of life, environment damage, transportation system disruption, or economic disruption in a particular area. 46 U.S.C. § 70101(6).

²³DHS determines the level of risk faced by U.S. port areas and then assigns those port areas to one of three groups based on that risk. There are seven Group I port areas that are considered critical.

²⁴33 C.F.R. § 103.300.

The area maritime security committees, in consultation with applicable stakeholders within their geographic region, are to assist the Coast Guard in developing the port area maritime security plans. Each area maritime security plan is to describe the area and infrastructure covered by the plan, establish area response and recovery protocols for a transportation security incident, and include any other information DHS requires.²⁵ In addition, during the development of each plan, the Coast Guard is to develop a risk-based security assessment that includes the identification of the critical infrastructure and operations in the port, a threat assessment, and a vulnerability and consequence assessment, among other things.²⁶ The assessment is also to consider, among other things, physical security of infrastructure and operations of the port, existing security systems available to protect maritime personnel, and radio and telecommunication systems, including computer systems and networks as well as other areas that may, if damaged, pose a risk to people, infrastructure, or operations within the port. Upon completion of the assessment, a written report must be prepared that documents the assessment methodology that was employed, describes each vulnerability²⁷ identified and the resulting consequences,²⁸ and provides risk reduction strategies that could be used for continued operations in the port.

MTSA and its associated regulations also require port facility owners and operators to develop facility security plans for the purpose of preparing certain maritime facilities, such as container terminals and chemical processing plants, to deter a transportation security incident.²⁹ The plans are to be updated at least every 5 years and are expected to be consistent with the port's area maritime security plan. The MTSA implementing regulations require that the facility security plans document

²⁵46 U.S.C. § 70103(b); see also 33 C.F.R. §§ 103.500-103.520.

²⁶See 33 C.F.R. §§ 103.400-103.410. A security system is defined as a device or multiple devices designed, installed, and operated to monitor, detect, observe, or communicate about activity that may pose a security threat in a location or locations on a vessel or facility. 33 C.F.R. § 101.105.

²⁷Vulnerability is defined as a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

²⁸A consequence is defined as an effect of an event, incident, or occurrence.

²⁹46 U.S.C. § 70103(c); see also 33 C.F.R. §§ 105.400-105.415.

information on security systems and communications, as well as facility vulnerability and security measures, among other things. The implementing regulations also require port facility owners and operators, as well as their designated facility security officers, to ensure that a facility security assessment is conducted and that, upon completion, a written report is included with the corresponding facility security plan submission for review and approval by the captain of the port.³⁰ The facility security assessment report must include an analysis that considers measures to protect radio and telecommunications equipment, including computer systems and networks, among other things.

Enacted in October 2006, the SAFE Port Act created and codified new programs and initiatives related to the security of the U.S. ports, and amended some of the original provisions of MTSA. For example, the SAFE Port Act required the Coast Guard to establish a port security exercise program.³¹

Port Security Grant Funding

MTSA also codified the Port Security Grant Program, which is to help defray the costs of implementing security measures at domestic ports.³² According to MTSA, funding is to be directed towards the implementation of area maritime security plans and facility security plans among port authorities, facility operators, and state and local government agencies that are required to provide port security services. Port areas use funding from the grant program to improve port-wide risk management, enhance maritime domain awareness, and improve port recovery and resiliency efforts through developing security plans, purchasing security equipment, and providing security training to employees. FEMA is responsible for designing and operating the administrative mechanisms needed to implement and manage the grant program. Coast Guard officials provide subject matter expertise regarding the maritime industry to FEMA to inform grant award decisions.

³⁰See 33 C.F.R. §§ 105.300-105.310.

³¹6 U.S.C. § 912.

³²The Port Security Grant Program was established in January 2002 when the Transportation Security Administration was appropriated \$93.3 million to award grants to critical national seaports. Pub. L. No. 107-117, 115 Stat. 2230, 2327 (2002). In November 2002, MTSA codified the program. 46 U.S.C. § 70107. Since fiscal year 2002, the appropriations acts have provided annual appropriations for the program.

Federal Stakeholders Have Taken Limited Actions to Address Cybersecurity in the Maritime Port Environment

DHS and the other stakeholders have taken limited steps with respect to maritime cybersecurity. In particular, the Coast Guard did not address cybersecurity threats in a 2012 national-level risk assessment. In addition, area maritime security plans and facility security plans provide limited coverage of cybersecurity considerations. While the Coast Guard helped to establish mechanisms for sharing security-related information, the degree to which these mechanisms were active and facilitated the sharing of cybersecurity-related information varied. Also, FEMA had taken steps to address cybersecurity through the Port Security Grant Program, but it has not taken additional steps to help ensure cyber-related risks are effectively addressed. Other federal stakeholders have also taken some actions to address cybersecurity in the maritime environment. According to DHS officials, a primary reason for limited efforts in addressing cyber-related threats in the maritime environment is that the severity of cyber-related threats has only recently been recognized. Until the Coast Guard and FEMA take additional steps to more fully implement their efforts, the maritime port environment remains at risk of not adequately considering cyber-based threats in its mitigation efforts.

The Coast Guard Did Not Address Cyber-Related Risks in a National-Level Risk Assessment for the Maritime Mode

While the Coast Guard has assessed risks associated with physical threats to port environments, these assessments have not considered risks related to cyber threats. NIPP recommends sector-specific agencies and critical infrastructure partners manage risks from significant threats and hazards to physical and cyber critical infrastructure for their respective sectors through, among other things, the

- identification and detection of threats and hazards to the nation's critical infrastructure;
- reduction of vulnerabilities of critical assets, systems, and networks; and
- mitigation of potential consequences to critical infrastructure if incidents occur.

The Coast Guard completes, on a biennial basis, the National Maritime Strategic Risk Assessment, which is to be an assessment of risk within the maritime environment and risk reduction based on the agency's efforts. Its results are to provide a picture of the risk environment, including a description of the types of threats the Coast Guard is expected to encounter within its areas of responsibility, such as ensuring the security of port facilities, over the next 5 to 8 years. The risk assessment is also to be informed by numerous inputs, such as historical

incident and performance data, the views of subject matter experts, and risk models, including the Maritime Security Risk Analysis Model.³³

However, the Coast Guard did not address cybersecurity in the fourth and latest iteration of the National Maritime Strategic Risk Assessment, which was issued in 2012. While the assessment contained information regarding threats, vulnerabilities, and the mitigation of potential risks in the maritime environment, none of the information addressed cyber-related risks. The Coast Guard attributed this gap to its limited efforts to develop inputs related to cyber threats, vulnerabilities, and consequences to inform the assessment. Additionally, Coast Guard officials stated that the Maritime Security Risk Analysis Model, a key input to the risk assessment, did not contain information regarding cyber-related threats, vulnerabilities, and potential impacts of cyber incidents. The Coast Guard plans to address this deficiency in the next iteration of the assessment, which is expected to be completed by September 2014, but officials could provide no details on how cybersecurity would be specifically addressed.

Without a thorough assessment of cyber-related threats, vulnerabilities, and potential consequences to the maritime subsector, the Coast Guard has limited assurance that the maritime mode is adequately protected against cyber-based threats. Assessments of cyber risk would help the Coast Guard and other maritime stakeholders understand the most likely and severe types of cyber-related incidents that could affect their operations and use this information to support planning and resource allocation to mitigate the risk in a coordinated manner. Until the Coast Guard completes a thorough assessment of cyber risks in the maritime environment, maritime stakeholders will be less able to appropriately plan and allocate resources to protect the maritime transportation mode.

³³The Maritime Security Risk Analysis Model is the primary tool employed by the Coast Guard to assess and manage security risks in the maritime domain. Using a combination of target and attack mode scenarios, this tool assesses risk in terms of threat, vulnerability, and consequences. The tool enables area maritime security committees to perform detailed scenario risk assessments on the entire maritime critical infrastructure. The maritime mode uses the program to inform strategic and tactical risk decision making. In November 2011, we reported on the approach, use, and efforts to measure this model in GAO, *Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations*, [GAO-12-14](#) (Washington D.C.: Nov. 17, 2011).

Maritime-Related Security Plans Provide Limited Coverage of Cybersecurity Considerations

MTSA and the SAFE Port Act provide the statutory framework for preventing, protecting against, responding to, and recovering from a transportation security incident in the maritime environment. MTSA requires maritime stakeholders to develop security documentation, including area maritime security plans and facility security plans. These plans, however, do not fully address the cybersecurity of their respective ports and facilities.

Area maritime security plans do not fully address cyber-related threats, vulnerabilities, and other considerations. The three area maritime security plans we reviewed from the three high-risk port areas we visited generally contained very limited, if any, information about cyber-related threats and mitigation activities. For example, the three plans reviewed included information about the types of information and communications technology systems that would be used to communicate security information to prevent, manage, and respond to a transportation security incident; the types of information that are considered to be Sensitive Security Information; and how to securely handle and transmit this information to those with a need to know.

However, the MTSA-required plans did not identify or address any other potential cyber-related threats directed at or vulnerabilities in the information and communications systems or include cybersecurity measures that port area stakeholders should take to prevent, manage, and respond to cyber-related threats and vulnerabilities. Coast Guard officials we met with agreed that the current set of area maritime security plans, developed in 2009, do not include cybersecurity information. This occurred in part because, as Coast Guard officials stated, the guidance for developing area maritime security plans did not require the inclusion of a cyber component. As a result, port area stakeholders may not be adequately prepared to successfully manage the risk of cyber-related transportation security incidents.

Coast Guard officials responsible for developing area maritime security plan guidance stated that the implementing policy and guidance for developing the next set of area maritime security plans includes basic considerations that maritime stakeholders should take into account to address cybersecurity. Currently, the area maritime security plans are formally reviewed and approved on a 5-year cycle, so the next updates will occur in 2014 and will be based on recently issued policy and guidance. Coast Guard officials stated that the policy and guidance for developing the area security plans was updated and promulgated in July 2013 and addressed inclusion of basic cyber components. Examples

include guidance to identify how the Coast Guard will communicate with port stakeholders in a cyber-degraded environment, the process for reporting a cyber-related breach of security, and direction to take cyber into account when developing a port's "all hazard"-compatible Marine Transportation System Recovery Plan. Our review of the guidance confirmed that it instructs preparers to generally consider cybersecurity issues related to information and communication technology systems when developing the plans. However, the guidance does not include any information related to the mitigation of cyber threats.

Officials representing both the Coast Guard and nonfederal entities that we met with stated that the current facility security plans also do not contain cybersecurity information. Our review of nine facility security plans from the organizations we met with during site visits confirmed that those plans generally have very limited cybersecurity information. For example, two of the plans had generic references to potential cyber threats, but did not have any specific information on assets that were potentially vulnerable or associated mitigation strategies. According to federal and nonfederal entities, this is because, similar to the guidance for the area security plans, the current guidelines for facility security plans do not explicitly require entities to include cybersecurity information in the plans. Coast Guard officials stated that the next round of facility security plans, to be developed in 2014, will include cybersecurity provisions. Since the plans are currently in development, we were unable to determine the degree to which cybersecurity information will be included.

Without the benefit of a national-level cyber-related risk assessment of the maritime infrastructure to inform the development of the plans, the Coast Guard has limited assurance that maritime-related security plans will appropriately address cyber-related threats and vulnerabilities associated with transportation security incidents.

Information-Sharing Mechanisms Were Active and Shared Cybersecurity Information to Varying Degrees

Although the Coast Guard helped to establish mechanisms for sharing security-related information, the degree to which these mechanisms were active and shared cybersecurity-related information varied. As the DHS agency responsible for maritime critical infrastructure protection-related efforts, the Coast Guard is responsible for establishing public-private partnerships and sharing information with federal and nonfederal entities in the maritime community. This information sharing is to occur through formalized mechanisms called for in federal plans and policy. Specifically, federal policy establishes a framework that includes government coordinating councils—composed of federal, state, local, or tribal

agencies—and encourages the voluntary formation of sector coordinating councils, typically organized, governed by, and made up of nonfederal stakeholders. Further, federal policy also encourages sector-specific agencies to promote the formulation of information sharing and analysis centers (ISAC), which are to serve as voluntary mechanisms formed by owners and operators for gathering, analyzing, and disseminating information on infrastructure threats and vulnerabilities among owners and operators of the sectors and the federal government.

The Maritime Modal Government Coordinating Council was established in 2006 to enable interagency coordination on maritime security issues. Coast Guard officials stated that the primary membership consisted of representatives from the Departments of Homeland Security, Transportation, Commerce, Defense, and Justice. Coast Guard officials stated that the council has met since 2006, but had only recently begun to discuss cybersecurity issues. For example, at its January 2013 annual meeting, the council discussed the implications of Executive Order 13636 for improving critical infrastructure cybersecurity for the maritime mode. In addition, during the January 2014 meeting, Coast Guard officials discussed efforts related to the development of a risk management framework that integrates cyber and physical security resilience efforts.

In 2007, the Maritime Modal Sector Coordinating Council, consisting of owners, operators, and associations from within the sector, was established to enable coordination and information sharing within the sector and with government stakeholders. However, the council disbanded in March 2011 and is no longer active. Coast Guard officials attributed the demise of the council to a 2010 presidential memorandum that precluded the participation of registered lobbyists in advisory committees and other boards and commissions, which includes all Critical Infrastructure Partnership Advisory Council bodies, including the Critical Infrastructure Cross-Sector Council, and all sector coordinating councils, according to DHS.³⁴ The former chair of the council stated that a majority of the members were registered lobbyists, and, as small trade associations, did not have non-lobbyist staff who could serve in this role.

³⁴See Presidential Memorandum on Lobbyists on Agency Boards and Commissions, Daily Comp. Pres. Docs., 2010 DCPD No. 00513 (June 18, 2010).

The Coast Guard has attempted to reestablish the sector coordinating council, but has faced challenges in doing so. According to Coast Guard officials, maritime stakeholders that would likely participate in such a council had viewed it as duplicative of statutorily authorized mechanisms, such as the National Maritime Security Advisory Committee³⁵ and area maritime security committees.³⁶ As a result, Coast Guard officials stated that there has been little stakeholder interest in reconstituting the council.

While Coast Guard officials stated that these committees, in essence, meet the information-sharing requirements of NIPP and, to some extent, may expand the NIPP construct into real world “all hazards” response and recovery activities, these officials also stated that the committees do not fulfill all the functions of a sector coordinating council. For example, a key function of the council is to provide national-level information sharing and coordination of security-related activities within the sector. In contrast, the activities of the area maritime security committees are generally focused on individual port areas. In addition, while the National Maritime Security Advisory Committee is made up of maritime-related private-sector stakeholders, its primary purpose is to advise and make recommendations to the Secretary of Homeland Security so that the government can take actions related to securing the maritime port environment. Similarly, another primary function of the sector coordinating council may include identifying, developing, and sharing information concerning effective cybersecurity practices, such as cybersecurity working groups, risk assessments, strategies, and plans. Although Coast

³⁵See 46 U.S.C. § 70112. The National Maritime Security Advisory Committee operates in accordance with the Federal Advisory Committee Act, to advise, consult with, and make recommendations to the Secretary of Homeland Security, via the Commandant of the Coast Guard, on matters relating to maritime security. In September 2013, we observed a meeting of the committee at which the Coast Guard provided an update on recent cybersecurity efforts. For example, the Coast Guard discussed recent outreach efforts to educate and encourage industry and maritime partners to obtain training on cybersecurity. In addition, the Coast Guard provided an overview of cybersecurity-related efforts in working groups mandated by Executive Order 13636, which focused on a variety of activities, including identifying cyber-dependent elements of the maritime subsector. (See app. II for more information on efforts related to the executive order.)

³⁶See 33 C.F.R. § 103.300. The area maritime security committees have been established for each of 43 port areas to serve as maritime security-related information-sharing forums. Public and private industry partners from each port area make up the committees’ membership. Coast Guard officials stated that the working relationships developed through these committees typically foster daily interaction between committee members and the Coast Guard’s captain of the port.

Guard officials stated that several of the area maritime security committees had addressed cybersecurity in some manner,³⁷ the committees do not provide a national-level perspective on cybersecurity in the maritime mode. Coast Guard officials could not demonstrate that these committees had a national-level focus to improve the maritime port environment's cybersecurity posture.

In addition, the Maritime Information Sharing and Analysis Center was to serve as the focal point for gathering and disseminating information regarding maritime threats to interested stakeholders; however, Coast Guard officials could not provide evidence that the body was active or identify the types of cybersecurity information that was shared through it. They stated that they fulfill the role of the ISAC through the use of Homeport—a publicly accessible and secure Internet portal that supports port security functionality for operational use. According to the officials, Homeport serves as the Coast Guard's primary communications tool to support the sharing, collection, and dissemination of information of various classification levels to maritime stakeholders. However, the Coast Guard could not show the extent to which cyber-related information was shared through the portal.

Though the Coast Guard has established various mechanisms to coordinate and share information among government entities at a national level and between government and private stakeholders at the local level, it has not facilitated the establishment of a national-level council, as recommended by NIPP. The absence of a national-level sector coordinating council increases the risk that critical infrastructure owners and operators would not have a mechanism through which they can identify, develop, and share information concerning effective cybersecurity practices, such as cybersecurity working groups, risk assessments, strategies, and plans. As a result, the Coast Guard would not be aware of and thus not be able to mitigate cyber-based threats.

³⁷ Although officials stated that several of the 43 committees have established cybersecurity subcommittees and several others have held in-depth cybersecurity-related discussions, officials were unable to demonstrate the extent to which information on cyber-based threats, vulnerabilities, and implications to ports were addressed by and shared among the committees.

Port Security Grant Program Provides Some Guidance for Cybersecurity Grants but Has Not Taken Additional Steps to Help Ensure Risks are Addressed

Under the Port Security Grant Program, FEMA has taken steps to address cybersecurity in port areas by identifying enhancing cybersecurity capabilities as a funding priority in fiscal years 2013 and 2014 and by providing general guidance regarding the types of cybersecurity-related proposals eligible for funding. DHS annually produces guidance that provides the funding amounts available under the program for port areas and information about eligible applicants, the application process, and funding priorities for that fiscal year, among other things. Fiscal year 2013 and 2014 guidance stated that DHS identified enhancing cybersecurity capabilities as one of the six priorities for selection criteria for all grant proposals in these funding cycles.³⁸ FEMA program managers stated that FEMA added projects that aim to enhance cybersecurity capabilities as a funding priority in response to the issuance of Presidential Policy Directive 21 in February 2013.³⁹

Specifically, the 2013 guidance stated that grant funds may be used to invest in functions that support and enhance port-critical infrastructure and key resources in both physical space and cyberspace under Presidential Policy Directive 21. The 2014 guidance expanded on this guidance to encourage applicants to propose projects to aid in the implementation of the National Institute of Standards and Technology's cybersecurity framework, established pursuant to Executive Order 13636, and provides a hyperlink to additional information about the framework. In addition, the guidance refers applicants to the just-established DHS Critical Infrastructure Cyber Community Voluntary Program for resources

³⁸In fiscal years 2013 and 2014, the guidance identified the following funding priorities for proposals: (1) enhancing maritime domain awareness; (2) enhancing improvised explosive device and chemical, biological, radiological, and nuclear explosives prevention, protection, response and supporting recovery capabilities; (3) enhancing cybersecurity capabilities; (4) port resilience and supporting recovery capabilities; (5) training and exercises; and (6) equipment associated with Transportation Worker Identification Credential implementation. Allowable costs under the fiscal years 2013 and 2014 Port Security Grant Program include efforts to build and sustain core capabilities across the Prevention, Protection, Mitigation, Response and Recovery mission areas essential to achieving the National Preparedness Goal. Cybersecurity is one of the core capabilities.

³⁹Prior to the release of Executive Order 13636 (February 19, 2013), DHS guidance for the grant program did not identify projects that enhance cybersecurity capabilities as one of its funding priorities.

to assist critical infrastructure owners and operators in the adoption of the framework and managing cyber risks.⁴⁰

While these actions are positive steps towards addressing cybersecurity in the port environment, FEMA has not consulted individuals with cybersecurity-related subject matter expertise to assist with the review of cybersecurity-related proposals. Program guidance states that grant applications are to undergo a multi-level review for final selection,⁴¹ including a review by a National Review Panel, comprised of subject matter experts drawn from the Departments of Homeland Security and Transportation.⁴² However, according to FEMA program managers, the fiscal year 2013 National Review Panel did not include subject matter experts from DHS cybersecurity and critical infrastructure agencies—such as the DHS Office of Cybersecurity and Communications, the DHS Office of Infrastructure Protection, or the Coast Guard’s Cyber Command. As a result, the National Review Panel had limited subject matter expertise to evaluate and prioritize cybersecurity-related grant proposals for funding.

⁴⁰According to program documentation, DHS launched the Critical Infrastructure Cyber Community Voluntary Program in February 2014 to coincide with the release of the cybersecurity framework.

⁴¹Specifically, according to FEMA guidance, the proposal review and selection process consists of three levels: an initial review, a field review, and a national-level review. During the initial review, FEMA officials review grant proposals for completion. During the field review, Coast Guard captains of the port, in coordination with officials of the Department of Transportation’s Maritime Administration, review and score proposals according to (1) the degree to which a proposal addresses program goals, including enhancing cybersecurity capabilities, and (2) the degree to which a proposal addresses one of the area maritime security plan priorities (e.g., transportation security incident scenarios), among other factors. The captains of the port provide a prioritized list of eligible projects for funding within each port area to FEMA, which coordinates the national review process.

⁴²Specifically, according to FEMA guidance, the national review consists of the following steps: (1) The National Review Panel conducts an initial review of the prioritized project lists for each port area to determine whether the proposed projects would accomplish intended risk mitigation goals. (2) The National Review Panel validates and normalizes the prioritized list of projects from the captains of the port and provides a master list of prioritized projects by port area. (3) A risk-based analysis is then applied to the National Review Panel’s validated and prioritized lists for each port area. The risk-based analysis considers factors such as the captain of the port ranking, the relationship of the projects to one or more of the national port security priorities, and the risk level of the port area in which the project would be located, among other factors. (4) The National Review Panel evaluates and validates the consolidated and ranked project list resulting from application of the risk-based analysis and submits its determinations to FEMA. The Secretary of Homeland Security has the final approval authority for all projects.

In March 2014, FEMA program managers stated that cybersecurity experts were not involved in the National Review Panel in part because the panel has been downsized in recent years. For the future, the officials stated that FEMA is considering revising the review process to identify cybersecurity proposals early on in the review process in order to obtain relevant experience and expertise from the Coast Guard and other subject matter experts to inform proposal reviews. However, FEMA has not documented this new process or its procedures for the Coast Guard and FEMA officials at the field and national review levels to follow for the fiscal year 2014 and future cycles.

In addition, because the Coast Guard has not conducted a comprehensive risk assessment for the maritime environment that includes cyber-related threats, grant applicants and DHS officials have not been able to use the results of such an assessment to inform their grant proposals, project scoring, and risk-based funding decisions. MTSA states that, in administering the program, national economic and strategic defense concerns based on the most current risk assessments available shall be taken into account.⁴³ Further, according to MTSA, Port Security Grant Program funding is to be used to address Coast Guard-identified vulnerabilities, among other purposes. FEMA officials stated that the agency considers port risk during the allocation and proposal review stages of the program funding cycle.⁴⁴ However, FEMA program managers stated that the risk formula and risk-based analysis that FEMA uses in the allocation and proposal review stages do not assess cyber threats and vulnerabilities.

Additionally, during the field-level review, captains of the port score grant proposals according to (1) the degree to which a proposal addresses program goals, including enhancing cybersecurity capabilities, and (2) the degree to which a proposal addresses one of the area maritime security

⁴³See 46 U.S.C. § 70107(a).

⁴⁴Specifically, DHS is required by law to allocate program funding according to risk. 46 U.S.C. § 70107(a). In the allocation stage of the program, FEMA uses a risk formula to place port areas into port groupings according to risk of terrorist attacks. During the proposal review stage, the guidance states that FEMA applies a risk-based analysis to the National Review Panel's validated and prioritized lists for each port area in all groups. The risk-based analysis considers factors such as the captain of the port ranking, the relationship of the projects to one or more of the national port security priorities, and the risk level of the port area in which the project would be located, among other factors.

plan priorities (e.g., transportation security incident scenarios), among other factors. However, as Coast Guard officials stated, and our review of area maritime security plans indicated, current area maritime security plans generally contain very limited, if any, information about cyber-related threats. Further, a FEMA Port Security Grant Program section chief stated that he was not aware of a risk assessment for the maritime mode that discusses cyber-related threats, vulnerabilities, and potential impact. Using the results of such a maritime risk assessment that fully addresses cyber-related threats, vulnerabilities, and consequences, which—as discussed previously—has not been conducted, to inform program guidance could help grant applicants and reviewers more effectively identify and select projects for funding that could enhance the cybersecurity of the nation’s maritime cyber infrastructure.

Furthermore, FEMA has not developed or implemented outcome measures to evaluate the effectiveness of the Port Security Grant Program in achieving program goals, including enhancing cybersecurity capabilities. As we reported in November 2011, FEMA had not evaluated the effectiveness of the Port Security Grant Program in strengthening critical maritime infrastructure because it had not implemented measures to track progress toward achieving program goals.⁴⁵ Therefore, we recommended that FEMA—in collaboration with the Coast Guard—develop time frames and related milestones for implementing performance measures to monitor the effectiveness of the program. In response, in February 2014 FEMA program managers stated that the agency developed and implemented four management and administrative measures in 2012 and two performance measures to track the amount of funds invested in building and sustaining capabilities in 2013.⁴⁶ According to a FEMA program manager, FEMA did not design the two performance measures to evaluate the effectiveness of the program in addressing

⁴⁵GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*, [GAO-12-47](#) (Washington, D.C.: Nov. 17, 2011).

⁴⁶The four management and administrative measures are (1) the percentage of preparedness grant awards processed within 120 days, (2) the percentage of preparedness grant awards monitored programmatically, (3) the percentage of grant funds released to grantees within 270 days, and (4) the percentage of preparedness grant awards closed within 90 days. The two performance measures are the percentage of program funding invested in building new capabilities and the percentage of funding invested in sustaining existing capabilities. According to FEMA officials, in fiscal year 2013, 53 percent of program funding was used to build new capabilities and 47 percent was used to sustain existing capabilities.

individual program goals, such as enhancing cybersecurity capabilities, but to gauge the program's effectiveness in reducing overall maritime risk in a port area based on program funding. While these measures can help improve FEMA's management of the program by tracking how funds are invested, they do not measure program outcomes.

In addition, in February 2012, we found that FEMA had efforts under way to develop outcome measures for the four national preparedness grant programs, including the Port Security Grant Program, but that it had not completed these efforts.⁴⁷ Therefore, we recommended that FEMA revise its plan in order to guide the timely completion of ongoing efforts to develop and implement outcome-based performance measures for all four grant programs. In January 2014, FEMA officials stated that they believe that the implementation of project-based grant application tracking and reporting functions within the Non-Disaster Grant Management System will address our February 2012 recommendation that the agency develop outcome measures to determine the effectiveness of the Port Security Grant Program.⁴⁸ However, the officials did not provide details about how these functions will address the recommendation.

While the development of the Non-Disaster Grant Management System is a positive step toward improving the management and administration of preparedness grants, FEMA officials stated that the deployment of these system functions has been delayed due to budget reductions, and the time frame for building the project-based applications and reporting functions is fiscal year 2016. Therefore, it is too early to determine how FEMA will use the system to evaluate the effectiveness of the Port Security Grant Program. Until FEMA develops outcome measures to evaluate the effectiveness of the program in meeting program goals, it cannot provide reasonable assurance that funds invested in port security grants, including those intended to enhance cybersecurity capabilities, are strengthening critical maritime infrastructure—including cyber-based infrastructure—against risks associated with potential terrorist attacks and other incidents.

⁴⁷GAO, *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, [GAO-12-303](#) (Washington, D.C.: Feb. 28, 2012).

⁴⁸The Non-Disaster Grant Management System is a web-based system under development that is intended to provide FEMA and its stakeholders with a system that supports the grants management life cycle and consolidates grants information.

Other Federal Agencies Have Taken Actions to Address Cybersecurity in the Maritime Port Environment

In addition to DHS, the 2010 Transportation Systems Sector-Specific Plan identified the Departments of Commerce, Defense, Justice, and Transportation as members of the Maritime Modal Government Coordinating Council. Many agencies, including others within DHS, had taken some actions with respect to the cybersecurity of the maritime subsector. For more details on these actions, see appendix II.

Conclusions

Disruptions in the operations of our nation's ports, which facilitate the import and export of over \$1.3 trillion worth of goods annually, could be devastating to the national economy. While the impact of a physical event (natural or manmade) appears to have been better understood and addressed by maritime stakeholders than cyber-based events, the growing reliance on information and communications technology suggests the need for greater attention to potential cyber-based threats.

Within the roles prescribed for them by federal law, plans, and policy, the Coast Guard and FEMA have begun to take action. In particular, the Coast Guard has taken action to address cyber-based threats in its guidance for required area and facility plans and has started to leverage existing information-sharing mechanisms. However, until a comprehensive risk assessment that includes cyber-based threats, vulnerabilities, and consequences of an incident is completed and used to inform the development of guidance and plans, the maritime port sector remains at risk of not adequately considering cyber-based risks in its mitigation efforts. In addition, the maritime sector coordinating council is currently defunct, which may limit efforts to share important information on threats affecting ports and facilities on a national level. Further, FEMA has taken actions to enhance cybersecurity through the Port Security Grant Program by making projects aimed at enhancing cybersecurity one of its funding priorities. However, until it develops procedures to instruct grant reviewers to consult cybersecurity-related subject matter experts and uses the results of a risk assessment that identifies any cyber-related threats and vulnerabilities to inform its funding guidance, FEMA will be limited in its ability to ensure that the program is effectively addressing cyber-related risks in the maritime environment.

Recommendations for Executive Action

To enhance the cybersecurity of critical infrastructure in the maritime sector, we recommend that the Secretary of Homeland Security direct the Commandant of the Coast Guard to take the following actions:

-
- work with federal and nonfederal partners to ensure that the maritime risk assessment includes cyber-related threats, vulnerabilities, and potential consequences;
 - use the results of the risk assessment to inform how guidance for area maritime security plans, facility security plans, and other security-related planning should address cyber-related risk for the maritime sector; and
 - work with federal and nonfederal stakeholders to determine if the Maritime Modal Sector Coordinating Council should be reestablished to better facilitate stakeholder coordination and information sharing across the maritime environment at the national level.

To help ensure the effective use of Port Security Grant Program funds to support the program's stated mission of addressing vulnerabilities in the maritime port environment, we recommend that the Secretary of Homeland Security direct the FEMA Administrator to take the following actions:

- in coordination with the Coast Guard, develop procedures for officials at the field review level (i.e., captains of the port) and national review level (i.e., the National Review Panel and FEMA) to consult cybersecurity subject matter experts from the Coast Guard and other relevant DHS components, if applicable, during the review of cybersecurity grant proposals for funding and
- in coordination with the Coast Guard, use any information on cyber-related threats, vulnerabilities, and consequences identified in the maritime risk assessment to inform future versions of funding guidance for grant applicants and reviews at the field and national levels.

Agency Comments and Our Evaluation

We provided a draft of this report to the Departments of Homeland Security, Commerce, Defense, Justice, and Transportation for their review and comment. DHS provided written comments on our report (reprinted in app. IV). In its comments, DHS concurred with our recommendations. In addition, the department stated that the Coast Guard is working with a variety of partners to determine how cyber-related threats, vulnerabilities, and potential consequences are to be addressed in the maritime risk assessment, which the Coast Guard will use to inform security planning efforts (including area maritime security plans and facility security plans). DHS also stated that the Coast Guard will continue to promote the re-establishment of a sector coordinating council, and will also continue to use existing information-sharing

mechanisms. However, DHS did not provide an estimated completion date for these efforts.

In addition, DHS stated that FEMA will work with the Coast Guard to develop the recommended cyber consultation procedures for the Port Security Grant Program by the end of October 2014, and will use any information on cyber-related threats, vulnerabilities, and consequences from the maritime risk assessment in future program guidance, which is scheduled for publication in the first half of fiscal year 2015.

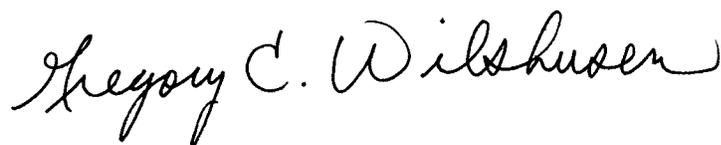
Officials from DHS and the Department of Commerce also provided technical comments via e-mail. We incorporated these comments where appropriate. Officials from the Departments of Defense, Justice, and Transportation stated that they had no comments.

We are sending copies of this report to interested congressional committees; the Secretaries of Commerce, Defense, Homeland Security, and Transportation; the Attorney General of the United States; the Director of Office of Management and Budget; and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Stephen L. Caldwell at (202) 512-9610 or caldwells@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may

be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix V.

Sincerely yours,

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive style with a large initial 'G'.

Gregory C. Wilshusen
Director, Information Security Issues

A handwritten signature in black ink that reads "Stephen L. Caldwell". The signature is written in a cursive style with a large initial 'S'.

Stephen L. Caldwell
Director, Homeland Security and Justice Issues

Appendix I: Objective, Scope, and Methodology

Our objective was to identify the extent to which the Department of Homeland Security (DHS) and other stakeholders have taken steps to address cybersecurity in the maritime port environment.

The scope of our audit focused on federal agencies that have a role or responsibilities in the security of the maritime port environment, to include port facilities. We focused on the information and communications technology used to operate port facilities. We did not include other aspects of the maritime environment such as vessels, off-shore platforms, inland waterways, intermodal connections, systems used to manage water-based portions of the port, and federally managed information and communication technology.

To identify federal agency roles and select the organizations responsible for addressing cybersecurity in the maritime port environment, we reviewed relevant federal law, regulations, policy, and critical infrastructure protection-related strategies, including the following:

- Homeland Security Act of 2002;
- Maritime Transportation Security Act of 2002;
- Homeland Security Presidential Directive 7—Critical Infrastructure Identification, Prioritization, and Protection, December 2003;
- Security and Accountability for Every Port Act of 2006;
- 2006 National Infrastructure Protection Plan;
- 2009 National Infrastructure Protection Plan;
- 2013 National Infrastructure Protection Plan;
- 2010 Transportation Systems Sector-Specific Plan;
- Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, February 12, 2013;
- Executive Order 13636—Improving Critical Infrastructure Cybersecurity; and
- Title 33, Code of Federal Regulations, Chapter 1, Subchapter H.

We analyzed these documents to identify federal agencies responsible for taking steps to address cybersecurity in the maritime environment, such as developing a risk assessment and information-sharing mechanisms, guiding the development of security plans in response to legal requirements, and providing financial assistance to support maritime port security activities. Based on our analysis, we determined that the U.S. Coast Guard (Coast Guard) and Federal Emergency Management Agency (FEMA), within DHS, were relevant to our objective. We also included the Departments of Transportation, Defense, Commerce, and Justice as they were identified as members of the Maritime Modal Government Coordinating Council in the 2010 Transportation Systems

Sector-Specific Plan. We also included other DHS components, such as U.S. Customs and Border Protection, National Protection and Programs Directorate, Transportation Security Administration, and United States Secret Service, based on our prior cybersecurity and port security work and information learned from interviews during our engagement.

To determine the extent to which the Coast Guard and FEMA have taken steps to address cybersecurity in the maritime port environment, we collected and analyzed relevant guidance and reports. For example, we analyzed the Coast Guard's 2012 National Maritime Strategic Risk Assessment, Coast Guard guidance for developing area maritime security plans, the 2012 Annual Progress Report—National Strategy for Transportation Security, the Transportation Sector Security Risk Assessment, and FEMA guidance for applying for and reviewing proposals under the Port Security Grant Program.¹ We also examined our November 2011 and February 2012 reports related to the Port Security Grant Program and our past work related to FEMA grants management for previously identified issues and context.² In addition, we gathered and analyzed documents and interviewed officials from DHS's Coast Guard, FEMA, U.S. Customs and Border Protection, Office of Cybersecurity and Communications, Office of Infrastructure Protection, Transportation Security Administration, and United States Secret Service; the Department of Commerce's National Oceanic and Atmospheric Administration; the Department of Defense's Transportation Command; the Department of Justice's Federal Bureau of Investigation; and the Department of Transportation's Maritime Administration, Office of Intelligence, Security and Emergency Response, and the Volpe Center.

To gain an understanding of how information and communication technology is used in the maritime port environment and to better understand federal interactions with nonfederal entities on cybersecurity

¹DHS, Federal Emergency Management Agency, *FY 2013 and FY 2014 Port Security Grant Program (PSGP) Funding Opportunity Announcements*.

²See GAO, *Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened*, [GAO-12-47](#) (Washington, D.C.: Nov. 17, 2011); *Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs*, [GAO-12-303](#) (Washington, D.C.: Feb. 28, 2012); and *Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act*, [GAO-12-1009T](#) (Washington, D.C.: Sept. 11, 2012), among others listed in "Related GAO Products" at the end of this report.

issues, we conducted site visits to three port areas—Houston, Texas; Los Angeles/Long Beach, California; and New Orleans, Louisiana. These ports were selected in a non-generalizable manner based on their identification as both high risk (Group I) ports by the Port Security Grant Program,³ and as national leaders in calls by specific types of vessels—oil and natural gas, containers, and dry bulk—in the Department of Transportation Maritime Administration’s March 2013 report, *Vessel Calls Snapshot, 2011*. For those port areas, we analyzed the appropriate area maritime security plans for any cybersecurity-related information.

We also randomly selected facility owners from Coast Guard data on those facilities required to prepare facility security plans under the Maritime Transportation Security Act’s implementing regulations. For those facilities whose officials agreed to participate in our review, we interviewed staff familiar with Coast Guard facility security requirements or information technology security, and analyzed their facility security plans for any cybersecurity-related items. We also included additional nonfederal entities such as port authorities and facilities as part of our review. The results of our analysis of area maritime security plans and facility security plans at the selected ports cannot be projected to other facilities at the port areas we visited or other port areas in the country. We also met with other port stakeholders, such as port authorities and an oil storage and transportation facility. We met with the following organizations:

- APM Terminals
- Axiall
- Cargill
- Domino Sugar Company
- Harris County, Texas, Information Technology Center
- Louisiana Offshore Oil Port
- Magellan Terminals Holdings, L.P.
- Metropolitan Stevedoring
- Port of Houston Authority
- Port of Long Beach
- Port of Los Angeles
- Port of New Orleans

³The program uses a risk model to group port areas into risk of terrorist attack. Group I port areas have been determined to be the highest risk. For more information, see [GAO-12-47](#).

- SSA Marine
- St. Bernard Port
- Trans Pacific Container Service

We determined that information provided by the federal and nonfederal entities, such as the type of information contained within the area maritime security plans and facility security plans, was sufficiently reliable for the purposes of our review. To arrive at this assessment, we corroborated the information by comparing the plans with statements from relevant agency officials.

We conducted this performance audit from April 2013 to June 2014 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix II: Additional Federal Maritime Cybersecurity Actions

This appendix summarizes cybersecurity-related actions, if any, taken by other agencies of the departments identified as members of the Government Coordinating Council of the Maritime Mode related to the nonfederally owned and operated maritime port environment.

The Department of Homeland Security

Integrated Task Force

Under Executive Order 13636, the Secretary of Homeland Security is to use a risk-based approach to identify critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security. The Secretary is also to apply consistent, objective criteria in identifying such critical infrastructure. Sector-specific agencies were to provide the Secretary with information necessary to identify such critical infrastructure.

To implement Executive Order 13636, DHS established an Integrated Task Force to, among other things, lead DHS implementation and coordinate interagency and public- and private-sector efforts. One of the eight working groups that made up the task force was assigned the responsibility for identifying cyber-dependent infrastructure. Officials from DHS's Office of Infrastructure Protection who were responsible for the working group stated that, using the defined methodology, the task force examined the maritime mode as part of its efforts.

National Protection and Programs Directorate

Office of Cybersecurity and Communications

The Office of Cybersecurity and Communications, among other things, is responsible for collaborating with public, private, and international partners to ensure the security and continuity of the nation's cyber and communications infrastructures in the event of terrorist attacks, natural disasters, and catastrophic incidents.

One division of the Office of Cybersecurity and Communications (Stakeholder Engagement and Cyber Infrastructure Resilience) offers to partner with critical infrastructure partners—including those in the maritime port environment—to conduct cyber resilience reviews. These reviews are voluntary and are based on the CERT® Resilience Management Model, a process improvement model for managing operational resilience. They are facilitated by field-based Cyber Security

Advisors. The primary goal of this program is to evaluate how critical infrastructure and key resource providers manage the cybersecurity of significant information.

In addition, the Industrial Control Systems Cyber Emergency Response Team—a branch of the National Cybersecurity and Communications Integration Center division within the Office of Cybersecurity and Communications—directed the development of the Cyber Security Evaluation Tool, which is a self-assessment tool that evaluates the cybersecurity of an automated industrial control or business system using a hybrid risk- and standards-based approach, and provides relevant recommendations for improvement.

We observed one maritime port entity engage with Office of Cybersecurity and Communications staff members to conduct a cyber resilience review. According to data provided by Office of Cybersecurity and Communications officials, additional reviews have been conducted with maritime port entities. In addition, three maritime port entities informed us they conducted a self-assessment using the Cyber Security Evaluation Tool.

Office of Infrastructure Protection

The Office of Infrastructure Protection is responsible for working with public- and private-sector critical infrastructure partners and leads the coordinated national effort to mitigate risk to the nation's critical infrastructure. Among other things, the Office of Infrastructure Protection has the overall responsibility for coordinating implementation of NIPP across 16 critical infrastructure sectors and overseeing the development of 16 sector-specific plans.

Through its Protective Security Coordination Division, the Office of Infrastructure Protection also has a network of field-based protective security advisors, who are security experts that serve as a direct link between the department and critical infrastructure partners in the field. Two nonfederal port stakeholders identified protective security advisors as a resource for assistance in cybersecurity issues.

Officials from Infrastructure Protection's Strategy and Policy Office supported the Coast Guard in developing the sector-specific plan and annual report for the maritime mode.

U.S. Customs and Border
Protection

U.S. Customs and Border Protection (CBP) is responsible for securing America's borders. This includes ensuring that all cargo enters the United States legally, safely, and efficiently through official sea ports of entry; preventing the illegal entry of contraband into the country at and between ports of entry; and enforcing trade, tariff, and intellectual property laws and regulations.

In addition, CBP developed and administered the Customs-Trade Partnership Against Terrorism program, a voluntary program where officials work in partnership with private companies to review the security of their international supply chains and improve the security of their shipments to the United States. Under this program, CBP issued minimum security criteria for U.S.-based marine port authority and terminal operators that include information technology security practices (specifically, password protection, establishment of information technology security policies, employee training on information technology security, and developing a system to identify information technology abuse that includes improper access).

United States Secret Service

Among other things, the Secret Service protects the President, Vice President, visiting heads of state and government, and National Special Security Events; safeguards U.S. payment and financial systems; and investigates cyber/electronic crimes. In support of these missions, the Secret Service has several programs that have touched on maritime port cybersecurity.

The Electronic Crimes Task Force initiative is a network of task forces established in the USA PATRIOT Act for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payments systems.

The Secret Service also conducts Critical Systems Protection advances for protective visits. This program identifies, assesses, and mitigates any risks posed by information systems to persons and facilities protected by the Secret Service. It also conducts protective advances to identify, assess, and mitigate any issues identified with networks or systems that could adversely affect the physical security plan or cause physical harm to a protectee. The advances support all of the Secret Service's protective detail offices by implementing network monitoring, and applying cyber intelligence analysis. Additionally, the program supports full spectrum protective visits, events, or venues domestically, in foreign countries, special events, and national special security events.

In addition, Secret Service personnel in Los Angeles have engaged with maritime port stakeholders in Los Angeles and Long Beach in several ways. For example, Secret Service staff gave a general cybersecurity threat presentation to port stakeholders, though no specific cyber threats to the maritime port environment were discussed. In addition, Secret Service was requested by a local governmental entity to assist in assessing the cyber aspects of critical infrastructure. Secret Service officials stated that they are still very early on in this process and are currently working with the entity to identify the critical assets/components of the cyber infrastructure. The process is still in the information-gathering phase, and officials do not expect to release any sort of summary product until mid-2014 at the earliest. Officials stated that the end product would detail any potential vulnerabilities identified during the assessment and make recommendations for mitigation that the stakeholder could implement if it chooses.

Secret Service officials also stated that an evaluation was conducted under the Critical Systems Protection Program with a maritime port stakeholder in the Houston area, but did not provide details regarding this evaluation.

Transportation Security Administration

The Transportation Security Administration (TSA) is the former lead sector-specific agency for the transportation systems sector. TSA currently co-leads the sector with the Department of Transportation and Coast Guard, and it supports, as needed, the Coast Guard's lead for maritime security. TSA also uses the Transportation Sector Security Risk Assessment to determine relative risks for the transportation modes. However, according to TSA officials, Coast Guard and TSA agreed in 2009 that the maritime modal risk assessment would be addressed in a separate report.

TSA also established the Transportation Systems Sector Cybersecurity Working Group, whose meetings (under the Critical Infrastructure Partnership Advisory Council framework) have discussed maritime cybersecurity issues.

The Department of Commerce

Although components of the Department of Commerce do have maritime-related efforts under way, none are directly related to the cybersecurity of the port environment. Further, the National Institute of Standards and Technology (NIST) has not developed any specific standards related to the cybersecurity of maritime facilities within our scope.

NIST has started to work with private sector stakeholders from different critical infrastructure sectors to develop a voluntary framework for reducing cyber risks to critical infrastructure, as directed by Executive Order 13636. It is developing this voluntary framework in accordance with its mission to promote U.S. innovation and industrial competitiveness. The framework has been shaped through ongoing public engagement. According to officials, more than 3,000 people representing diverse stakeholders in industry, academia, and government have participated in the framework's development through attendance at a series of public workshops and by providing comments on drafts. On February 12, 2014, NIST released the cybersecurity framework. Though representatives from numerous critical infrastructure sectors provided comments on the draft framework, only one maritime entity provided feedback, in October 2013. The entity stated that the framework provided a minimum level of cybersecurity information, but may not provide sufficient guidance to all relevant parties who choose to implement its provisions and suggestions. Additionally, the entity stated that it found the framework to be technical in nature and that it does not communicate at a level helpful for business executives. Department of Commerce officials stated that NIST worked to address these comments in the final version of the framework.

The Department of Transportation

The mission of the Department of Transportation is to serve the United States by ensuring a fast, safe, efficient, accessible, and convenient transportation system that meets our vital national interest and enhances the quality of life of the American people. The department is organized into several administrations, including the Research and Innovative Technology Administration, which coordinates the department's research programs and is charged with advancing the deployment of cross-cutting technologies to improve the nation's transportation networks. The administration includes the Volpe Center, which partners with public and private organizations to assess the needs of the transportation community, evaluate research and development endeavors, assist in the deployment of state-of-the-art transportation technologies, and inform decision- and policy-making through analyses. Volpe is funded by sponsoring organizations.

In 2011, Volpe entered into a 2-year agreement with DHS's Control Systems Security Program to evaluate the use of control systems in the transportation sector, including the maritime mode. Under this agreement, Volpe and DHS developed a road map to secure control systems in the transportation sector in August 2012. The document discussed the use of industrial control systems in the maritime mode, and described high-level

threats. It also established several goals for the entire transportation sector with near- (0-2 years), mid- (2-5 years), and long-term (5-10 years) objectives, metrics, and milestones. Volpe and DHS also developed a cybersecurity standards strategy for transportation industrial control systems, which identified tasks for developing standards for port industrial control systems starting in 2015. Volpe also conducted outreach to various maritime entities. According to Volpe officials, this study was conducted mostly at international port facilities and vessels (though U.S. ports were visited under a different program). The officials stated that the agreement was canceled due to funding reductions resulting from the recent budget sequestration.

DHS officials gave two reasons why funding for Volpe outreach was terminated after sequestration. First, as part of a reorganization of the Office of Cybersecurity and Communications, there is a heightened focus on “operational” activities, and DHS characterized Volpe’s assistance under the agreement as outreach and awareness. Second, the officials stated that because the demand for incident management and response continues to grow, a decision was made to stop funding Volpe to meet spending cuts resulting from sequestration and increase funding for cyber incident response for critical infrastructure asset owners and operators who use industrial control systems.

The Department of Justice

Although components of the Department of Justice have some efforts under way, most of those efforts occur at the port level. Specifically, the department’s Federal Bureau of Investigation is involved in several initiatives at the local level, focused on interfacing with key port stakeholders as well as relevant entities with state and local governments. These initiatives are largely focused on passing threat information to partners. Additionally, the Bureau’s Infragard program provides a forum to share threat information with representatives from all critical infrastructure sectors, including maritime.

The Department of Defense

While the Department of Defense has recognized the significance of cyber-related threats to maritime facilities, the department has no explicit role in the protection of critical infrastructure within the maritime sub-sector. Officials also said that the department had not supported maritime mode stakeholders regarding cybersecurity. In addition, though the Department of Defense was identified as a member of the Maritime Modal Government Coordinating Council in the 2010 Transportation Systems Sector-Specific Plan, the department was not listed as a participant in the

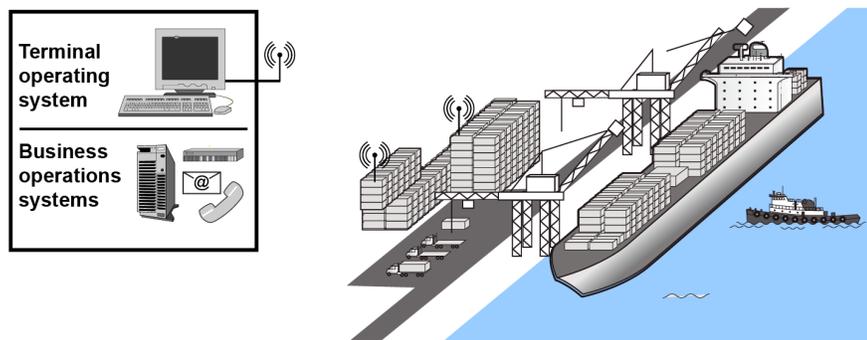
2013 or 2014 council meetings. Further, DHS, including the U.S. Coast Guard, had not requested support from Defense on cybersecurity of commercial maritime port operations and facilities.

Appendix III: Full Text for Figure 1 on Examples of Technologies Used in Maritime Port Environments

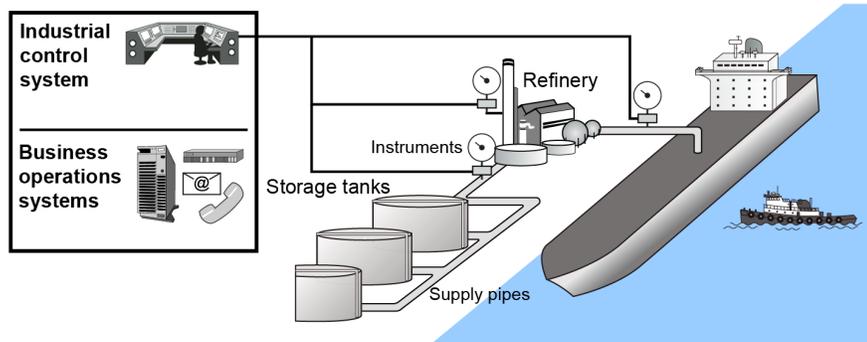
Figure 2 provides an overview of the technologies used in the maritime port environment (see interactive fig. 1) and includes the figure's rollover information.

Figure 2: Examples of Technologies Used in Maritime Port Environments (Printable Version)

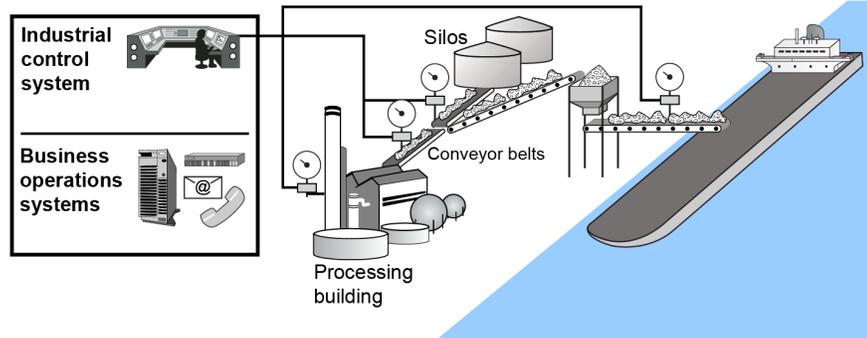
Container



Bulk liquid



Dry bulk



Source: GAO analysis of maritime sector information; Art Explosion (clip art).

Appendix IV: Comments from the Department of Homeland Security

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



**Homeland
Security**

May 23, 2014

Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

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

Re: Draft Report GAO-14-459, "MARITIME CRITICAL INFRASTRUCTURE PROTECTION: DHS Needs to Better Address Port Cybersecurity"

Dear Messrs. Wilshusen and Caldwell:

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

The Department is pleased to note GAO's recognition of the U.S. Coast Guard's (USCG) efforts to establish mechanisms for sharing security-related information and steps the Federal Emergency Management Agency (FEMA) has taken to address cybersecurity through the Port Security Grant Program. DHS is committed to considering cyber-based threats as part of its risk assessment process and in its mitigation efforts to enhance the cybersecurity of critical infrastructure in the maritime sector.

The draft report contained five recommendations with which the Department concurs. Specifically, GAO recommended that the Secretary of Homeland Security direct the Commandant of the Coast Guard to:

Recommendation 1: Work with federal and nonfederal partners to ensure that the maritime risk assessment includes cyber-related threats, vulnerabilities, and potential consequences.

Response: Concur. The USCG Director of Inspections and Compliance (CG-5PC) is already working with DHS, security experts, and interagency and industry partners to determine how best to ensure that the maritime risk assessment includes cyber-related threats, vulnerabilities and potential consequences. Physical port security poses a wide variety of challenges and threats emanating from the global cybersecurity arena add a

dimension of complexity that requires deliberative consideration. Estimated Completion Date (ECD): To be Determined (TBD).

Recommendation 2: Use the results of the risk assessment to inform how guidance for area maritime security plans, facility security plans, and other security-related planning should address cyber-related risk for the maritime sector.

Response: Concur. USCG CG-5PC will lead efforts to determine how to incorporate the results of risk assessments in guidance for area maritime security plans, facility security plans, and other security-related planning once the risk assessment process has been modified, as appropriate, and results are available for use. ECD: TBD.

Recommendation 3: Work with federal and nonfederal stakeholders to determine if the Maritime Modal Sector Coordinating Council should be reestablished to better facilitate stakeholder coordination and information-sharing across the maritime environment at the national level.

Response: Concur. The USCG CG-5PC will continue to promote the re-establishment of a Sector Coordinating Council (SCC). To date, CG-5PC has facilitated recurring Maritime SCC discussions with the Maritime Government Coordinating Council as well as the National Maritime Security Advisory Committee (NMSAC). CG-5PC has also solicited participation in an SCC through the sharing portal HOMEPORT.

In addition to promoting the re-establishment of an SCC, the USCG will continue to use other existing and effective information sharing mechanisms including the information sharing portal HOMEPORT, Area Maritime Security (AMS) Committees, the National Maritime Security Advisory Committee, Port Readiness Committees, Carrier and Trade Support Groups, the U.S. Computer Emergency Readiness Team, the Homeland Security Information Network-Critical Sectors, and the Common Assessment and Reporting Tool. The USCG supports the re-establishment of an SCC; however, it is an industry decision whether to establish this body. USCG will facilitate further discussions of this concept among industry partners, as appropriate. ECD: TBD.

GAO also recommended that the Secretary of Homeland Security direct the FEMA Administrator to:

Recommendation 4: In coordination with the Coast Guard, develop procedures for officials at the field review level (i.e., captains of the port) and national review level (i.e., the National Review Panel and FEMA) to consult cybersecurity subject matter experts from the Coast Guard and other relevant DHS components, if applicable, during the review of cybersecurity grant proposals for funding.

Response: Concur. FEMA's Preparedness Grants Division (GPD) will, in coordination with the USCG, develop procedures for officials at the field review level (i.e. Captains of the Port) and national review level (i.e. the National Review Panel and FEMA) to consult cybersecurity

subject matter experts from the USCG and other relevant DHS components, if applicable, during the review of cybersecurity grant proposals for funding. ECD: October 31, 2014.

Recommendation 5: In coordination with the Coast Guard, use any information on cyber-related threats, vulnerabilities, and consequences identified in the maritime risk assessment to inform future versions of funding guidance for grant applicants and reviews at the field and national levels.

Response: Concur. FEMA GPD will use any information on cyber-related threats, vulnerabilities and consequences identified in the maritime risk assessment to inform future versions of funding guidance for grant applicants and reviews at the field and national levels. Specially, FEMA will incorporate such information, as appropriate, in future versions of related guidance publications. The next cycle for publication of guidance updates is scheduled for first half of FY 2015. ECD: March 31, 2015.

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

Sincerely,



Jim H. Crumpacker, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Appendix V: GAO Contacts and Staff Acknowledgments

GAO Contacts

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

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

Staff Acknowledgments

In addition to the contacts named above, key contributions to this report were made by Michael W. Gilmore (Assistant Director), Christopher Conrad (Assistant Director), Bradley W. Becker, Jennifer L. Bryant, Franklin D. Jackson, Tracey L. King, Kush K. Malhotra, Lee McCracken, Umesh Thakkar, and Adam Vodraska.

Related GAO Products

National Preparedness: FEMA Has Made Progress, but Additional Steps Are Needed to Improve Grant Management and Assess Capabilities. [GAO-13-637T](#). Washington, D.C.: June 25, 2013.

Communications Networks: Outcome-Based Measures Would Assist DHS in Assessing Effectiveness of Cybersecurity Efforts. [GAO-13-275](#). Washington, D.C.: April 3, 2013.

High Risk Series: An Update. [GAO-13-283](#). Washington, D.C.: February 14, 2013.

Cybersecurity: National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively Implemented. [GAO-13-187](#). Washington, D.C.: February 14, 2013.

Information Security: Better Implementation of Controls for Mobile Devices Should Be Encouraged. [GAO-12-757](#). Washington, D.C.: September 18, 2012.

Maritime Security: Progress and Challenges 10 Years after the Maritime Transportation Security Act. [GAO-12-1009T](#). Washington, D.C.: September 11, 2012.

Information Security: Cyber Threats Facilitate Ability to Commit Economic Espionage. [GAO-12-876T](#). Washington, D.C.: June 28, 2012.

IT Supply Chain: National Security-Related Agencies Need to Better Address Risks. [GAO-12-361](#). Washington, D.C.: March 23, 2012.

Homeland Security: DHS Needs Better Project Information and Coordination among Four Overlapping Grant Programs. [GAO-12-303](#). Washington, D.C.: February 28, 2012.

Critical Infrastructure Protection: Cybersecurity Guidance Is Available, but More Can Be Done to Promote Its Use. [GAO-12-92](#). Washington, D.C.: December 9, 2011.

Port Security Grant Program: Risk Model, Grant Management, and Effectiveness Measures Could Be Strengthened. [GAO-12-47](#). Washington, D.C.: November 17, 2011.

Coast Guard: Security Risk Model Meets DHS Criteria, but More Training Could Enhance Its Use for Managing Programs and Operations. [GAO-12-14](#). Washington, D.C.: November 17, 2011.

Information Security: Additional Guidance Needed to Address Cloud Computing Concerns. [GAO-12-130T](#). Washington, D.C.: October 6, 2011.

Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure. [GAO-11-865T](#). Washington, D.C.: July 26, 2011.

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. [GAO-10-628](#). Washington, D.C.: July 15, 2010.

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance. [GAO-10-606](#). Washington, D.C.: July 2, 2010.

Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment. [GAO-09-969](#). Washington, D.C.: September 24, 2009.

Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability. [GAO-08-588](#). Washington, D.C.: July 31, 2008.

Homeland Security: DHS Improved its Risk-Based Grant Programs' Allocation and Management Methods, But Measuring Programs' Impact on National Capabilities Remains a Challenge. [GAO-08-488T](#). Washington, D.C.: March 11, 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.

Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats. [GAO-07-705](#). Washington, D.C.: June 22, 2007.

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.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Phone

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

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

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

Connect with GAO

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

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

Public Affairs

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

