United States Government Accountability Office

Testimony

Before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, October 8, 2015

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Enhance Efforts to Address Port Cybersecurity

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

October 8, 2015

MARITIME CRITICAL INFRASTRUCTURE PROTECTION

DHS Needs to Enhance Efforts to Address Port Cybersecurity

GAO Highlights

Highlights of GAO-16-116T, a testimony before the Subcommittee on Border and Maritime Security, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The nation's maritime ports handle more than $1.3 trillion in cargo each year: a disruption at one of these ports could have a significant economic impact. Increasingly, port operations rely on computerized information and communications technologies, which can be vulnerable to cyber-based attacks. Federal entities, including DHS's Coast Guard and FEMA, have responsibilities for protecting ports against cyber-related threats. GAO has designated the protection of federal information systems as a government-wide high-risk area since 1997, and in 2003 expanded this to include systems supporting the nation's critical infrastructure.

This statement addresses (1) cyber-related threats facing the maritime port environment and (2) steps DHS has taken to address cybersecurity in that environment. In preparing this statement, GAO relied on work supporting its June 2014 report on cybersecurity at ports. (GAO-14-459)

What GAO Recommends

In its June 2014 report on port cybersecurity, GAO recommended that the Coast Guard include cyber-risks in its updated risk assessment for the maritime environment, address cyber-risks in its guidance for port security plans, and consider reestablishing the sector coordinating council. GAO also recommended that FEMA ensure funding decisions for its port security grant program are informed by subject matter expertise and a comprehensive risk assessment. DHS has partially addressed two of these recommendations since GAO's report was issued.

View GAO-16-116T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Similar to other critical infrastructures, the nation's ports face an evolving array of cyber-based threats. These can come from insiders, criminals, terrorists, or other hostile sources and may employ a variety of techniques or exploits, such as denial-of-service attacks and malicious software. By exploiting vulnerabilities in information and communications technologies supporting port operations, cyber-attacks can potentially disrupt the flow of commerce, endanger public safety, and facilitate the theft of valuable cargo.

In its June 2014 report, GAO determined that the Department of Homeland Security (DHS) and other stakeholders had taken limited steps to address cybersecurity in the maritime environment. Specifically:

- DHS's Coast Guard had not included cyber-related risks in its biennial assessment of risks to the maritime environment, as called for by federal policy. Specifically, the inputs into the 2012 risk assessment did not include cyber-related threats and vulnerabilities. Officials stated that they planned to address this gap in the 2014 revision of the assessment. However, when GAO recently reviewed the updated risk assessment, it noted that the assessments did not identify vulnerabilities of cyber-related assets, although it identified some cyber threats and their potential impacts.
- The Coast Guard also did not address cyber-related risks in its guidance for developing port area and port facility security plans. As a result, port and facility security plans that GAO reviewed generally did not include cyber threats or vulnerabilities. While Coast Guard officials noted that they planned to update the security plan guidance to include cyber-related elements, without a comprehensive risk assessment for the maritime environment, the plans may not address all relevant cyber-threats and vulnerabilities.
- The Coast Guard had helped to establish information-sharing mechanisms called for by federal policy, including a sector coordinating council, made up of private-sector stakeholders, and a government coordinating council, with representation from relevant federal agencies. However, these bodies shared cybersecurity-related information to a limited extent, and the sector coordinating council was disbanded in 2011. Thus, maritime stakeholders lacked a national-level forum for information sharing and coordination.
- DHS's Federal Emergency Management Agency (FEMA) identified enhancing cybersecurity capabilities as a priority for its port security grant program, which is to defray the costs of implementing security measures. However, FEMA's grant review process was not informed by Coast Guard cybersecurity subject matter expertise or a comprehensive assessment of cyber-related risks for the port environment. Consequently, there was an increased risk that grants were not allocated to projects that would most effectively enhance security at the nation's ports.

GAO concluded that until DHS and other stakeholders take additional steps to address cybersecurity in the maritime environment—particularly by conducting a comprehensive risk assessment that includes cyber threats, vulnerabilities, and potential impacts—their efforts to help secure the maritime environment may be hindered. This in turn could increase the risk of a cyber-based disruption with potentially serious consequences.

Chairman Miller, Ranking Member Vela, and Members of the Subcommittee:

Thank you for inviting me to testify at today's hearing on the risks of cyber attacks facing our nation's maritime facilities. As you know, maritime ports are an essential part of the United States' transportation critical infrastructure. They are an economic engine that handles more than $1.3 trillion in cargo each year. A major disruption in the maritime transportation system could have a significant impact on global shipping, international trade, and the global economy, as well as posing risks to public safety. This risk is heightened by ports' dependence on computer-reliant information and communication systems that may be vulnerable to cyber threats from various actors with malicious intent. Because of the increasing prevalence of cyber threats, since 1997 we have designated federal information security as a government-wide high-risk area, and in 2003 we expanded this to include the protection of systems supporting our nation's critical infrastructure.[1]

In my statement today, I will summarize the results of a report we issued in June 2014 on the extent to which the Department of Homeland Security (DHS) and other stakeholders have addressed cybersecurity in the maritime port environment.[2] Specifically, I will discuss (1) cyber-related threats facing the maritime port environment and (2) steps DHS and other stakeholders have taken to address cyber risks in the maritime environment, as well as provide updates on actions DHS has taken to implement recommendations we made in our report. More detailed information on our objective, scope, and methodology for that work can be found in the issued report.

The work on which this testimony is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[1]GAO'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. See most recently, GAO, *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: Feb. 11, 2015).

[2]GAO, *Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity*, GAO-14-459 (Washington, D.C.: June 5, 2014).

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 travels through these ports each day—including automobiles, grain, and millions of cargo containers. While no two ports are exactly alike, many share certain characteristics such as their size, proximity to a metropolitan area, the volume of cargo they process, and connections to complex transportation networks. These characteristics can make them vulnerable to physical security threats.

Moreover, entities within the maritime port environment are vulnerable to cyber-based threats because they rely on various types of information and communications technologies to manage the movement of cargo throughout the ports. These technologies include

- terminal operating systems, which are information systems used to, among other things, control container movements and storage;
- industrial control systems, which facilitate the movement of goods using conveyor belts or pipelines to structures such as refineries, processing plants, and storage tanks;
- business operations systems, such as e-mail and file servers, enterprise resources planning systems, networking equipment, phones, and fax machines, which support the business operations of the terminal; and
- access control and monitoring systems, such as camera surveillance systems and electronically enabled physical access control devices, which support a port's physical security and protect sensitive areas.

All of these systems are potentially vulnerable to cyber-based attacks and other threats, which could disrupt operations at a port.

Federal Policies and Laws Establish Requirements and Responsibilities for Protecting Maritime Critical Infrastructure

While port owners and operators are responsible for the cybersecurity of their operations, federal agencies have specific roles and responsibilities for supporting these efforts. The National Infrastructure Protection Plan (NIPP) establishes 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 federally designated critical infrastructure sectors (maritime is a component of one of these sectors—the transportation sector); 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.

The NIPP establishes a framework for operating and sharing information across and between federal and nonfederal stakeholders within each sector. These coordination activities are carried out through sector coordinating councils and government coordinating councils. Further, under the NIPP, each critical infrastructure sector is to develop a sector-specific plan that details the application of the NIPP risk management framework to the sector. As the sector-specific agency for the maritime mode of the transportation sector, the Coast Guard is to coordinate protective programs and resilience strategies for the maritime environment.

Further, Executive Order 13636, issued in February 2013, calls for various actions to improve the cybersecurity of critical infrastructure.[3] These include developing a cybersecurity framework; increasing the volume, timeliness, and quality of cyber threat information shared with the U.S. private sector; considering prioritized actions within each sector to promote cybersecurity; and identifying critical infrastructure for which a cyber incident could have a catastrophic impact.

More recently, the Cybersecurity Enhancement Act of 2014[4] further refined public-private collaboration on critical infrastructure cybersecurity by authorizing the National Institute of Standards and Technology to facilitate and support the development of a voluntary set of standards, guidelines, methodologies, and procedures to cost-effectively reduce cyber risks to critical infrastructure.

In addition to these cyber-related policies and law, there are laws and regulations governing maritime security. One of the primary laws is the Maritime Transportation Security Act of 2002 (MTSA)[5] which, along with its implementing regulations developed by the Coast Guard, requires a wide range of security improvements for the nation's ports, waterways, and coastal areas. DHS is the lead agency for implementing the act's provisions, and DHS component agencies, including the Coast Guard and the Federal Emergency Management Agency (FEMA), have specific responsibilities for implementing the act.

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

[4]Pub. L. No. 113-274 (Dec. 18, 2014).

[5]Pub. L. No. 107-295 (Nov. 25, 2002).

To carry out its responsibilities for the security of geographic areas around ports, the Coast Guard has designated a captain of the port within each of 43 geographically defined port areas. The captain of the port is responsible for overseeing the development of the security plans within each of these port areas. In addition, maritime security committees, made up of key stakeholders, are to identify critical port infrastructure and risks to the port areas, develop mitigation strategies for these risks, and communicate appropriate security information to port stakeholders. As part of their duties, these committees are to assist the Coast Guard in developing port area maritime security plans. The Coast Guard is to develop a risk-based security assessment during the development of the port area maritime security plans that considers, among other things, radio and telecommunications systems, including computer systems and networks that may, if damaged, pose a risk to people, infrastructure, or operations within the port.

In addition, under MTSA, owners and operators of individual port facilities are required to develop facility security plans to prepare certain maritime facilities, such as container terminals and chemical processing plants, for deterring a transportation security incident. The implementing regulations for these facility security plans require written security assessment reports to be included with the plans that, among other things, contain an analysis that considers measures to protect radio and telecommunications equipment, including computer systems and networks.

MTSA also codified the Port Security Grant Program, which is to help defray the costs of implementing security measures at domestic ports. Port areas use funding from this program to improve port-wide risk management, enhance maritime domain awareness, and improve port recovery and resilience efforts through developing security plans, purchasing security equipment, and providing security training to employees. FEMA is responsible for administering this program with input from Coast Guard subject matter experts.

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

Like threats affecting other critical infrastructures, threats to the maritime IT infrastructure are evolving and growing and can come from a wide array of sources. Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused

by, among other things, natural disasters, defective computer or network equipment, software coding errors, and careless or poorly trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled insiders, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or pursuing a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques—or exploits—that may adversely affect federal information, computers, software, networks, and operations, such as a denial of service, which prevents or impairs the authorized use of networks, systems, or applications.

Reported incidents highlight the impact that cyber attacks could have on the maritime environment, and researchers have identified security vulnerabilities in systems aboard cargo vessels, such as global positioning systems and systems for viewing digital nautical charts, as well as on servers running on systems at various ports.

In some cases, these vulnerabilities have reportedly allowed hackers to target ships and terminal systems. Such attacks can send ships off course or redirect shipping containers from their intended destinations. For example, according to Europol's European Cybercrime Center, a cyber incident was reported in 2013 (and corroborated by the FBI) in which malicious software was installed on a computer at a foreign port. The reported goal of the attack was to track the movement of 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.

DHS and Other Stakeholders Have Taken Limited Actions to Address Maritime Port Cybersecurity

In June 2014 we reported that DHS and the other stakeholders had taken limited steps with respect to maritime cybersecurity.[6] In particular, risk assessments for the maritime mode did not address cyber-related risks; maritime-related security plans contained limited consideration of cybersecurity; information-sharing mechanisms shared cybersecurity information to varying degrees; and the guidance for the Port Security Grant Program did not take certain steps to ensure that cyber risks were addressed.

Maritime Risk Assessment Did Not Address Cybersecurity

In its 2012 National Maritime Strategic Risk assessment, which was the most recent available at the time of our 2014 review, the Coast Guard did not address cyber-related risks to the maritime mode. As called for by the NIPP, the Coast Guard completes this assessment on a biennial basis, and it is to provide a description of the types of threats the Coast Guard expects to encounter within its areas of responsibility, such as ensuring the security of port facilities, over the next 5 to 8 years. The assessment is 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, which is a tool that assesses risk in terms of threat, vulnerability, and consequences.

However, we found that while the 2012 assessment contained information regarding threats, vulnerabilities, and the mitigation of potential risks in the maritime environment, none of the information addressed cyber-related risks or provided a thorough assessment of cyber-related threats, vulnerabilities, and potential consequences. Coast Guard officials attributed this gap to limited efforts to develop inputs related to cyber threats to inform the risk assessment. For example, the Maritime Security Risk Analysis Model did not contain information related to cyber threats. The officials noted that they planned to address this deficiency in the next iteration of the assessment, which was to be completed by September 2014, but did not provide details on how cybersecurity would be specifically addressed.

[6]GAO-14-459.

We therefore recommended that DHS direct the Coast Guard to ensure that the next iteration of the maritime risk assessment include cyber-related threats, vulnerabilities, and potential consequences. DHS concurred with our recommendation, and the September 2014 version of the National Maritime Strategic Risk Assessment identifies cyber attacks as a threat vector for the maritime environment and assigns some impact values to these threats. However, the assessment does not identify vulnerabilities of cyber-related assets. Without fully addressing threats, vulnerabilities, and consequences of cyber incidents in its assessment, the Coast Guard and its sector partners will continue to be hindered in their ability to appropriately plan and allocate resources for protecting maritime-related critical infrastructure.

Maritime Security Plans' Consideration of Cybersecurity Was Limited

As we reported in June 2014, maritime security plans required by MTSA did not fully address cyber-related threats, vulnerabilities, and other considerations. Specifically, three area maritime security plans we reviewed from three high-risk port areas contained very limited, if any, information about cyber-threats and mitigation activities. For example, the three plans 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 considered to be sensitive security information; and how to securely handle such information. They did not, however, identify or address any other potential cyber-related threats directed at or vulnerabilities in these systems or include cybersecurity measures that port-area stakeholders should take to prevent, manage, and respond to cyber-related threats and vulnerabilities.

Similarly, nine facility security plans from the nonfederal organizations we met with during our 2014 review generally had 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. Officials representing the Coast Guard and nonfederal entities acknowledged that their facility security plans at the time generally did not contain cybersecurity information.

Coast Guard officials and other stakeholders stated that the area and facility-level security plans did not adequately address cybersecurity because the guidance for developing the plans did not require a cyber component. Officials further stated that guidance for the next iterations of the plans, which were to be developed in 2014, addressed cybersecurity.

However, in the absence of a maritime risk environment that addressed cyber risk, we questioned whether the revised plans would appropriately address the cyber-related threats and vulnerabilities affecting the maritime environment.

Accordingly, we recommended that DHS direct the Coast Guard to use the results of the next maritime risk assessment to inform guidance for incorporating cybersecurity considerations for port area and facility security plans. While DHS concurred with this recommendation, as noted above, the revised maritime risk assessment does not address vulnerabilities of systems supporting maritime port operations, and thus is limited as a tool for informing maritime cybersecurity planning. Further, it is unclear to what extent the updated port area and facility plans include cyber risks because the Coast Guard has not yet provided us with updated plans.

Information-Sharing Mechanisms Varied in Sharing Cybersecurity Information

Consistent with the private-public partnership model outlined in the NIPP, the Coast Guard helped establish various collaborative bodies for sharing security-related information in the maritime environment. For example, the Maritime Modal Government Coordinating Council was established to enable interagency coordination on maritime security issues, and members included representatives from DHS, as well as the Departments of Commerce, Defense, Justice, and Transportation. Meetings of this council discussed implications for the maritime mode of the President's executive order on improving critical infrastructure cybersecurity, among other topics.

In addition, the Maritime Modal Sector Coordinating Council, consisting of owners, operators, and associations from within the sector, was established in 2007 to enable coordination and information sharing. However, this council disbanded in March 2011 and was no longer active, when we conducted our 2014 review. Coast Guard officials stated that maritime stakeholders had viewed the sector coordinating council as duplicative of other bodies, such as area maritime security committees, and thus there was little interest in reconstituting the council.

In our June 2014 report, we noted that in the absence of a sector coordinating council, the maritime mode lacked a body to facilitate national-level information sharing and coordination of security-related information. By contrast, maritime security committees are focused on specific geographic areas.

We therefore recommended that DHS direct the Coast Guard to work with maritime stakeholders to determine if the sector coordinating council

should be reestablished. DHS concurred with this recommendation, but has yet to take action on this. The absence of a national-level sector coordinating council increases that risk that critical infrastructure owners and operators will be unable to effectively share information concerning cyber threats and strategies to mitigate risks arising from them.

Port Security Grant Program Did Not Take Key Steps to Effectively Address Cyber Risks

In 2013 and 2014 FEMA identified enhancing cybersecurity capabilities as a funding priority for its Port Security Grant Program and provided guidance to grant applicants regarding the types of cybersecurity-related proposals eligible for funding. However, in our June 2014 report we noted that the agency's national review panel had not consulted with cybersecurity-related subject matter experts to inform its review of cyber-related grant proposals. This was partly because FEMA had downsized the expert panel that reviewed grants. In addition, because the Coast Guard's maritime risk assessment did not include cyber-related threats, grant applicants and reviewers were not able to use the results of such an assessment to inform grant proposals, project review, and risk-based funding decisions.

Accordingly, we recommended that DHS direct FEMA to (1) develop procedures for grant proposal reviewers, at both the national and field level, to consult with cybersecurity subject matter experts from the Coast Guard when making funding decisions and (2) use information on cyber-related threats, vulnerabilities, and consequences identified in the revised maritime risk assessment to inform funding guidance for grant applicants and reviewers.

Regarding the first recommendation, FEMA officials told us that since our 2014 review, they have consulted with the Coast Guard's Cyber Command on high-dollar value cyber projects and that Cyber Command officials sat on the review panel for one day to review several other cyber projects. FEMA officials also provided examples of recent field review guidance sent to the captains of the port, including instructions to contact Coast Guard officials if they have any questions about the review process. However, FEMA did not provide written procedures at either the national level or the port area level for ensuring that grant reviews are informed by the appropriate level of cybersecurity expertise. FEMA officials stated the fiscal year 2016 Port Security Grant Program guidance will include specific instructions for both the field review and national review as part of the cyber project review.

With respect to the second recommendation, since the Coast Guard's 2014 maritime risk assessment does not include information about cyber vulnerabilities, as discussed above, the risk assessment would be of limited value to FEMA in informing its guidance for grant applicants and reviewers. As a result, we continue to be concerned that port security grants may not be allocated to projects that will best contribute to the cybersecurity of the maritime environment.

In summary, protecting the nation's ports from cyber-based threats is of increasing importance, not only because of the prevalence of such threats, but because of the ports' role as conduits of over a trillion dollars in cargo each year. Ports provide a tempting target for criminals seeking monetary gain, and successful attacks could potentially wreak havoc on the national economy. The increasing dependence of port activities on computerized information and communications systems makes them vulnerable to many of the same threats facing other cyber-reliant critical infrastructures, and federal agencies play a key role by working with port facility owners and operators to secure the maritime environment. While DHS, through the Coast Guard and FEMA, has taken steps to address cyber threats in this environment, they have been limited and more remains to be done to ensure that federal and nonfederal stakeholders are working together effectively to mitigate cyber-based threats to the ports. Until DHS fully implements our recommendations, the nation's maritime ports will remain susceptible to cyber risks.

Chairman Miller, Ranking Member Vela, and Members of the Subcommittee, this concludes my prepared statement. I would be pleased to answer any questions you may have at this time.

Contact and Acknowledgments

If you or your staff have any questions about this testimony, please contact Gregory C. Wilshusen, Director, Information Security Issues at (202) 512-6244 or wilshuseng@gao.gov. GAO staff who made key contributions to this testimony are Michael W. Gilmore, Assistant Director; Bradley W. Becker; Jennifer L. Bryant; Kush K. Malhotra; and Lee McCracken.