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.