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.

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.