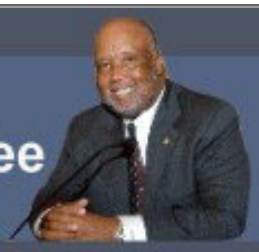
NEWS ALERT

U.S. HOUSE OF REPRESENTATIVES

Homeland Security Committee

Rep. Bennie G. Thompson, Ranking Member



FOR IMMEDIATE RELEASE

Statement of Ranking Member Bennie G. Thompson

Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber-Attack?

October 8, 2015 (Washington) – Today, Committee on Homeland Security Ranking Member Bennie G. Thompson (D-MS) delivered the following prepared remarks for the Border and Maritime Security subcommittee hearing entitled "Protecting Maritime Facilities in the 21st Century: Are Our Nation's Ports at Risk for a Cyber-Attack?"

"The Committee on Homeland Security has long been engaged on the issues of cybersecurity, port security, and critical infrastructure protection. This hearing brings those critical issues together by focusing on cybersecurity at America's ports.

A 2014 Government Accountability Office (GAO) report found that actions taken by the Department of Homeland Security (DHS) and other federal agencies to address cybersecurity in the maritime port environment have been limited. So much of the focus has been on improving the physical security at ports that cybersecurity at ports, an emerging threat, has been secondary.

In recent years, cyber technology has helped promote efficient port operations and enhanced security. But these benefits come with risks to the Maritime Transportation System. For example, in 2013, officials at Europol disclosed that a group of drug traffickers recruited hackers to breach information technology systems at the Port of Antwerp to smuggle container loads of cocaine.

Our cargo security programs are predicated on electronic transmission of manifest data, underscoring the potential risk of such cyber breaches not just from drug smugglers, but also other criminals and even terrorists. Requiring the Coast Guard to complete a cyber risk assessment and ensure that cyber risks are addressed in maritime security plans, as recommended by GAO, is a good first step toward reducing cyber vulnerabilities at ports.

Similarly, allowing Port Security Grant Program funds to be used for cybersecurity, and ensuring the funds are used effectively, is a step in the right direction. The Coast Guard's June 2015 Cyber Strategy presents cyberspace as another operational domain for the Service, and sets forth three strategic priorities: defending cyberspace, enabling operations, and protecting infrastructure.

I look forward to hearing from the Coast Guard today about how they intend to implement this Strategy, with the help of other government and private sector stakeholders. I also want to hear from GAO about what more can be done by DHS and the Coast Guard in this domain, as Coast Guard implements its Strategy.

Finally, I want to discuss with the ports how we can support their cybersecurity efforts, recognizing that each port is different and no single solution is likely to be appropriate for all. Certainly, providing ports and other stakeholders, like terminal operators and transportation companies, with the appropriate guidance and expertise will be essential. Adequate resources are also going to be necessary to address cybersecurity risks at ports, and Congress must provide those resources and help ensure they are used wisely."

# # #

FOR MORE INFORMATION: Please contact Adam Comis at (202) 225-9978