



**OPENING STATEMENT**

October 8, 2015

**MEDIA CONTACTS**

Susan Phalen, Matthew Ballard

**Statement of Subcommittee Chairman Candice Miller (R-MI)  
Border and Maritime Security Subcommittee  
House Homeland Security Committee**

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

Remarks as Prepared

Before we start, I would just like to offer my thoughts and prayers to the family of the 33 crewmembers of the El Faro, the cargo container ship that went missing last week near the Bahamas. I thank the men and women of the Coast Guard for their valiant efforts to find the ship and the missing crew.

The purpose of today's hearing is to examine the vulnerability of seaports to cyber-attacks and how well we are prepared to prevent and respond to such an attack.

Our meeting today marks the first Congressional hearing convened to examine cyber security at our nation's ports, which is fitting since October is also National Cybersecurity Awareness Month

The United States Coast Guard is the government agency responsible for the physical security of our nation's port infrastructure. Working through the Area Maritime Security Committees, the Coast Guard partners with port authorities and operators to update access controls, fence-off sensitive areas of the ports, and increase surveillance when appropriate.

Since the terrorist attacks of September 11, 2001, the United States Congress has appropriated \$2.4 billion dollars in port security grant funds to harden port facilities against the potential for a terror attack. As a nation, we have done a fairly good job updating the physical security at ports, but I am concerned that the U.S. government has fallen behind when it comes to the cyber security of the port.

Under the Maritime Transportation Security Act of 2002, the U.S. Coast Guard was granted responsibility for the protection of communication systems, including information that flows through the Marine Transportation System. Port facilities and ship operators, like many industries in America, increasingly rely on automation to streamline operations. While those innovations reduce the time it takes to stock our shelves, and lower the cost of doing business, they also carry risk.

Terror groups, nation-states, criminal organizations, hackers and even disgruntled employees could breach these systems – with potentially catastrophic results to the nation's economy.

More than \$1 trillion dollars of goods, from cars to oil to corn and everything in between move through the nation's seaports every year.

Increasingly, cargo is moving through our ports using automated industrial control systems. These computer systems are controlling machinery on ports to move containers, fill tanks and on-load and off-load ships.

I understand that the Port of Long Beach and port partners are working towards building perhaps the most automated and efficient container terminal in the United States. Once completed it will reduce wait times at the ports and increase throughput.

While this automation has substantial benefits, it does not come without risks. In 2014, a major U.S. port facility suffered a system disruption that shut down a significant number of ship-to-shore cranes for several hours. In Europe, drug smugglers attempted to hack into cargo tracking systems to rearrange containers and hide their drugs. Similarly, a foreign military is suspected of compromising several systems aboard a commercial ship contracted by the U.S. Transportation Command.

These breaches in the maritime domain are particularly concerning, not only from an economic standpoint, but because of the dangerous cargo such as Liquefied Natural Gas, and other Certain Dangerous Cargos that also pass through the nation's seaports. If a cyber-breach were to occur that tampered with the industrial control systems that monitor these cargos, it could potentially allow the release of harmful and dangerous chemicals.

Despite the fact the GAO has placed cyber security of our nation's critical infrastructure on the "High Risk" list since 2003, the Coast Guard, and DHS as a whole, have been slow to fully engage on cyber security efforts at the nation's 360 seaports.

The threat of cyber-attack is worrisome to be sure. But when it comes to the maritime domain and the protection of maritime critical infrastructure, who is really in charge?

The private sector owns the ports, and must clearly protect its own interests. However, the Department of Homeland Security must be involved to ensure communication between ports nationwide. Information sharing will undoubtedly be part of any solution as we look to protect our seaports and we must have a strategy that looks beyond individual ports.

Just as we have hardened physical security, we need to do the same in the virtual space for systems critical to the marine transportation system to protect against malicious actors. The first step in reducing this risk is to conduct risk assessments. The Coast Guard has not yet conducted cyber risk assessments, though some individual ports have taken the initiative themselves.

Port security grants can be a way to help port operators make wise choices based on an individual assessment of risk. In providing grant funding, however, we must understand which ports are at risk of a cyber incident. Retooling the Maritime Security Risk Analysis Model to incorporate cyber-risks is a concept worth exploring further and incorporating into the port security grant program.

Finally, I want to better understand how DHS, through the National Protection and Programs Directorate (NPPD) and the National Cybersecurity and Communication Integration Center, interfaces with the U.S. Coast Guard's cyber efforts.

We are all aware that the government moves slowly and this can cause us to quickly fall behind, especially in an area like cyber that moves rapidly.

With that in mind, should the Coast Guard's role in cyber be limited to oversight and prevention rather than the creation of standards?

This is a very technical field which may be outside the expertise of a Coast Guard Inspector. Therefore, despite the exposure to proprietary information, could third-party validators, authorized by the Coast Guard, review and certify cyber security standards? I think there is merit in looking at that model for cyber security and would be interested in hearing from the witnesses on that topic.

I thank the witnesses for appearing before us today and look forward to their testimony.

###