COMMITTEE ON HOMELAND SECURITY

Ranking Member Bennie G. Thompson

FOR IMMEDIATE RELEASE

Hearing Statement of Transportation & Maritime Security Subcommittee

Ranking Member Shri Thanedar (D-MI)

Port Cybersecurity: The Insidious Threat to U.S. Maritime Ports

February 29, 2024

The security of our Nation's seaports is vital to the success of our economy. Seaports move more than 99 percent of the cargo coming to the U.S. from overseas. They support more than 31 million American jobs and generate $5.4 trillion in total economic value, representing more than a quarter of the Nation's economy.

The daily life of Americans everywhere depends upon the ability of government experts, port owners and operators, and their partners and stakeholders to protect ports and the rest of the marine transportation system from both physical and cyberattacks. As ports have become increasingly networked and reliant on computer systems, the importance of instituting strong cybersecurity protections has risen dramatically.

We have already seen the devastating impacts cyberattacks on ports can have. Cyberattacks on ports in the U.S. and overseas have brought the transport of cargo to a standstill and cost hundreds of millions of dollars in economic damages. Thankfully, the Biden Administration is taking decisive action.

Just last week, the Administration announced a series of actions that will greatly enhance the cybersecurity of our Nation's ports. Last Wednesday, President Biden signed an Executive Order to provide the Coast Guard the express authority to address threats to cybersecurity and mitigate vulnerabilities. The Executive Order also requires maritime industry partners to report cyber incidents and threats to government agencies.

In addition, the Coast Guard issued proposed regulations to establish minimum cybersecurity requirements at U.S. seaports, covering a wide range of proven security measures to strengthen our cyber defenses. Finally, the Coast Guard issued a security directive to address vulnerabilities posed by Chinese-manufactured cranes, and President Biden announced an investment of more than $20 billion to improve port infrastructure and initiate domestic manufacturing of cranes.

Taken together, these actions represent the single largest advancement in port cybersecurity in history. These actions are just the latest in the Biden Administration's comprehensive approach to addressing longstanding cybersecurity threats to critical infrastructure. Following the Colonial Pipeline ransomware attack, the Administration committed to raising the cybersecurity baseline across all critical infrastructure sectors, including by using existing authorities to set baseline cybersecurity standards.

At President Biden's direction, the Department of Homeland Security initiated a series of "cybersecurity sprints," which encouraged key owners and operators in certain sectors to make security investments in partnership with the Federal government. These sprints leveraged DHS's resources and enhanced

cybersecurity across a wide range of critical areas. To date, these sprints have covered ransomware, the cybersecurity workforce, Industrial Control Systems, transportation, and election security.

In addition, the Transportation Security Administration has issued a series of important new security requirements addressing cybersecurity across a range of transportation modes, from pipelines, to mass transit and rail, to aviation. Last November, the Biden Administration announced the creation of the Supply Chain Resilience Center within DHS, which will help coordinate and advance efforts to secure chains from disruptions.

In addition to its sector-by-sector assessment of cybersecurity risks, the Biden Administration has taken seriously the growing threat posed by our most sophisticated adversaries. Notably, in April 2023, Secretary Mayorkas directed DHS to undertake a 90-day People's Republic of China Threats Sprint, which evaluated, among other things, security threats the People's Republic of China poses to U.S. supply chains. The Administration is taking bold action to address cybersecurity threats and vulnerabilities—not just for cranes and ports, but across all sectors of critical infrastructure. Now, it is time for Congress to do our part.

We sit here today on the verge of a potential government shutdown—yet again—because House Republicans have placed extreme political demands above their responsibility to govern. A government shutdown would be devastating to the Coast Guard's operations, including its efforts to implement cybersecurity enhancements.

# # #

Media contact: Adam Comis at 202-225-9978