Testimony

Eric Goldstein
Executive Assistant Director for Cybersecurity
Cybersecurity and Infrastructure Security Agency
U.S. Department of Homeland Security

FOR A HEARING ON

"Evaluating High-Risk Security Vulnerabilities At Our Nation's Ports"

BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

May 10, 2023

Chairman Giménez, Ranking Member Thanedar, and members of the Subcommittee: Thank you for the invitation to testify today on behalf of the Cybersecurity and Infrastructure Security Agency (CISA). CISA leads the national effort to understand, manage, and reduce risk to our critical infrastructure. This mission is grounded in partnership with each Sector Risk Management Agency and critical infrastructure operators in each sector. While each sector is uniquely critical, the Maritime Transportation Sub-Sector, and the nation's ports represented therein, serves as a linchpin of our nation's prosperity and security. For this reason, our work with the U.S. Coast Guard and the maritime community is uniquely essential. I appreciate this opportunity to discuss the cybersecurity elements of CISA's work on port security.

From Miami to Detroit, and from the Gulf Coast to the Pacific, America's ports drive our economic and national security. Maritime transportation accounts for the single largest share of U.S. trade, both supplying our households and businesses with necessities and facilitating trade that supports American jobs. We have seen in the past few years how disruptions to maritime commerce, regardless of cause, can produce significant impacts for businesses and consumers, and we recognize that America's ports are equally critical in enabling our armed forces to effectively deploy and supply.

At CISA, we share the Subcommittee's concern regarding threats to ports posed by the government of the People's Republic of China (PRC), which could manifest in multiple forms. We continue to work urgently with the Coast Guard and the port community to understand and mitigate these threats, whether from critical equipment manufactured by Chinese state-owned enterprises or the prospect of damaging cyber intrusions targeting port infrastructure. These threats catalyze our focus, clarify our intent, and underpin our shared investment.

Partnership with the United States Coast Guard and the Transportation Security Administration

Our nation's maritime system is highly complex, and no one organization maintains the authorities, resources, or capability to bear the burden of securing these systems alone. Our partnership with both the Coast Guard and the Transportation Security Administration (TSA) are foundational in achieving our shared mission. The Coast Guard and TSA play leading roles in operationalizing the Department of Homeland Security's responsibilities as a co-Sector Risk Management Agency for the Transportation Systems Sector. CISA coordinates with the Coast Guard and TSA to advance this work in several ways.

First, we must provide members of the maritime community, including port operators, with actionable information to protect their systems. For this reason, CISA and the Coast Guard frequently engage in joint amplification or development of combined products for this community, with recent examples including CISA's amplification of a Coast Guard Safety Alert

with recommended cybersecurity best practices for commercial vessels and a joint advisory regarding malware exploiting the Log4Shell vulnerability. In addition, the Coast Guard was a key partner in our development of the Cross-Sector Cybersecurity Performance Goals (CPGs), which provide a straightforward and actionable set of cybersecurity actions prioritized by cost, impact, and complexity and organized around the National Institute of Standards and Technology Cybersecurity Framework. The CPGs are a foundational tool to help any organization align limited cybersecurity resources toward the most impactful investments. We look forward to partnering closely with the Coast Guard to develop sector-specific goals for maritime stakeholders that reflect the unique technology and risk considerations of the sub-sector.

Second, the Coast Guard and TSA are key participants in Cyber Storm, CISA's annual national capstone cyber exercise that brings together the public and private sectors in a simulated response to a cyber crisis impacting the nation's critical infrastructure. During the current Cyber Storm exercise series, the Coast Guard and TSA are participating within working groups of federal entities to respond to a simulated cyber threat. These exercises foster collaboration and communication across agencies to ensure that federal and non-federal entities are ready to collectively respond to major cyber incidents.

Finally, CISA, the Coast Guard, and TSA coordinate through formal mechanisms to promote critical infrastructure security. All three agencies are members of the Maritime Modal Subsector Government Coordinating Council (GCC) under the Critical Infrastructure Partnership Advisory Council framework, which provides a forum for federal agencies to collaborate with one another and to seek private sector input. Specifically, the Maritime Modal Subsector GCC allows federal agencies to collaborate on strategies for mitigating risk to ports and other elements of the maritime transportation sub-sector. Through this coordinating council and other channels, CISA, the Coast Guard, and TSA stay connected with one another and with non-federal entities to support collective efforts to mitigate cybersecurity and other risks to ports.

Supporting Our Partners to Actively Reduce Risk

CISA also works directly with ports and other critical infrastructure entities to support their cybersecurity efforts. By leveraging our expertise, our ability to generate efficiencies of scale, and our ability to cross-reference information from multiple sources to gain broad visibility into the cyber threat environment, CISA is uniquely positioned to assist critical infrastructure operators with mitigating cybersecurity risk.

As a key part of this effort, we enable network owners and operators to harden their networks against known and potential tactics, techniques, and procedures used by PRC cyber actors. For example, we published in late 2022 a joint advisory with the National Security Agency and the Federal Bureau of Investigation outlining the vulnerabilities most frequently used by PRC actors, enabling organizations around the country to close down intrusion paths commonly used by the

PRC to achieve their strategic goals. We regularly scan over 5,000 federal, critical infrastructure, and state, local, tribal, and territorial (SLTT) partners' networks upon their request to identify the presence of these vulnerabilities and notify identified entities to prioritize urgent mitigation. More recently, we have undertaken an effort intended to make network owners and operators aware of the prevalence of devices produced by PRC-based vendors that are listed on the Federal Communications Commission's "Covered List," which, under the Secure and Trusted Communications Networks Act of 2021, pose an "unacceptable risk to the national security of the United States or the security and safety of United States persons." Using commercial tools, we have identified such products used on critical infrastructure networks across the country and have already notified 88 critical infrastructure organizations using such products about the potential associated risks. In nearly all cases, the notified entities have chosen to take urgent steps to replace these products from their networks and reduce the likelihood of unauthorized access by PRC actors.

We are particularly focused on proactive efforts to reduce the likelihood that our partner entities will experience serious cybersecurity incidents. We have enrolled a select group of our nation's most critical infrastructure entities in the CyberSentry program, a voluntary effort that uses commercial off-the-shelf tools and equipment to identify and detect malicious activity targeting critical infrastructure corporate and industrial control systems networks. This program has yielded significant operational benefits among participating entities, and we look forward to expanding into the maritime sub-sector in the next year. Further, our Vulnerability Scanning service helps organizations identify and address vulnerabilities, particularly those that are known to be exploited by adversaries. In addition, we have over 100 cybersecurity personnel across the country to provide guidance, assistance, and a front door to CISA's broader portfolio of risk reduction services. These regional personnel are working every day to build relationships with the maritime community to understand what these stakeholders need and ensure that CISA provides every possible resource to support their cybersecurity efforts.

CISA also has an important role in helping critical infrastructure entities prevent the worst outcomes after a cyber intrusion has occurred. We leverage information from partners and security researchers to notify victims so that they can take action to contain and eradicate the threat. Our new Pre-Ransomware Notification Initiative identifies organizations that ransomware actors have compromised and aims to notify them before their data is encrypted or stolen, with over 160 having been notified so far. Once we receive information about a compromised organization, our field personnel take urgent action to notify the victim organization and provide specific mitigation guidance. CISA also provides direct support to victims of cyber incidents through incident response services.

Looking to the future, CISA is continuously developing new capabilities to help our stakeholders drive down cyber risk based upon their feedback and needs. We are looking forward to several

impactful new efforts in the coming months, including an effort that will expand one of our cybersecurity shared service offerings beyond the federal sphere to certain critical infrastructure entities, a new attack surface management service, and a modernized cyber threat intelligence service. Through each of these efforts, we will work closely with the maritime community to understand their needs and maximize our ability to deliver services, information, and guidance that helps our partners detect, prevent, and effectively respond to cyber risks.

Getting Ahead of the Threat

Another pillar of CISA's cybersecurity work is our cybersecurity defense planning. This aligns with Congress's statutory direction for CISA to engage in joint planning with a range of critical infrastructure partners to create common, shoulder-to-shoulder approaches to confront malicious actors and significant cyber risks. To date, CISA's planning efforts have addressed topics including the cybersecurity implications of the Russian invasion of Ukraine and the creation of a framework for public-private crisis action planning. During 2023, CISA's planning agenda includes systemic risks posed by cyber intrusions against software and infrastructure that underlie multiple national critical functions, as well as updating the National Cyber Incident Response Plan. CISA will continue to engage transportation and maritime stakeholders in this work to ensure that it provides value for these key facets of our national infrastructure.

We take a strategic approach to reduce the likelihood of damaging intrusions, particularly those perpetrated by PRC actors. In so doing, we recognize a hard truth: most technology products used across American networks are neither secure by design nor by default, which makes it far too easy for malicious actors to find vulnerabilities and makes it far too hard for organizations to deploy necessary security measures. Recently we published a set of principles with six international partners that intends to catalyze progress toward further investments and cultural shifts necessary to achieve a safe and secure future. These principles aim for technology providers to take ownership of the security outcomes of their technology products, shifting the burden of security from the customers and ensuring executive level commitment for software manufacturers to prioritize security as a critical element of product development. This will be a long-term journey but a necessary one that will require all elements of society, from enterprises to technology providers to Congress, to join together in driving change.

Conclusion

Thank you again for this opportunity for CISA to testify on this important topic. I look forward to further discussion of how our Coast Guard and TSA partnership, our rapidly maturing capabilities, and our planning efforts advance the national imperative to secure our ports. I welcome any questions you may have.