TESTIMONY OF

Christa Brzozowski
Acting Assistant Secretary for Trade and Economic Security
Office of Strategy, Policy, and Plans
U.S. Department of Homeland Security

For a Hearing

BEFORE

United States House of Representatives
Committee on Homeland Security
Transportation and Maritime Security Subcommittee

ON

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

February 29, 2024
Washington, DC

Introduction:

Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the Subcommittee. Thank you for the opportunity to appear before you today to discuss the U.S Department of Homeland Security's (DHS or Department) role in securing maritime infrastructure and bolstering supply chain resilience against potential threats posed by the People's Republic of China (PRC).

The Department is deeply committed to its national and economic security missions. Across DHS, we work diligently to address all hazards that threaten our transportation systems, critical infrastructure, and the safe and lawful flow of goods and people. The dedicated men and women of the Department work every day to protect our ports, screen and vet goods and travelers, and help infrastructure owners and operators respond to the threats of today and prepare for the threats of tomorrow. DHS leverages the extensive authorities, data, and expertise from its operational Components in trade and travel facilities, physical and cyber security, and disaster response and preparedness to protect our vital trade infrastructure, ensure the safe and lawful flow of critical goods, and protect U.S. economic security.

Supply Chain Resilience Center:

Understanding the depth and breadth of the Department's expertise, authorities, and capabilities in the economic security realm, Secretary Mayorkas has challenged the Department to coordinate and enhance its supply chain resilience efforts. In 2022, the Secretary called upon the Homeland Security Advisory Council (HSAC) to recommend new ways that DHS can advance supply chain resilience leveraging the Department's expertise and authorities. On November 27, 2023, in response to a resulting HSAC recommendation, President Biden and Secretary Mayorkas announced the creation of the Supply Chain Resilience Center (SCRC or Center) within the Office of Strategy, Policy, and Plans, to enhance coordination of the Department's supply chain efforts.

To prepare for the next economic disruption, be it a pandemic, conflict, or adversary-led market distorting activity, DHS, through the SCRC, is identifying threats to supply chain resilience, addressing security vulnerabilities, and helping Americans prepare for and mitigate supply chain disruptions. To accomplish these goals, the SCRC is coordinating all the tools at the Department's disposal, including our wide range of Component authorities and capabilities, to bolster critical supply chain resilience. By placing the SCRC within the DHS Office of Strategy, Policy, and Plans, the aim is to ensure that our many efforts to advance supply chain resilience across the DHS enterprise are more than the sum of their parts. The SCRC will ensure that the DHS approach to supply chain resilience is holistic in scope and tightly coordinated with the private sector to co-develop practical mitigations that protect our economy.

As the Department's central supply chain coordinator, the SCRC will leverage data and intelligence resources to identify future threats to critical U.S. supply chain. In this vein, we are building a Watch Center concept that will use both publicly available information and government information feeds to provide early identification of emerging or ongoing threats. The current Watch Center provides daily situational briefs to my office's leadership that

synthesizes internal and external information sources. Concurrently, we are working closely with the Department's Office of Intelligence and Analysis and the broader U.S. Intelligence Community to ensure our leaders are up to date on the latest threats.

The SCRC is collaborating closely with our interagency partners to build supply chain resilience in critical infrastructure, to ensure our nation is better prepared for and able to respond to any threat. The SCRC will seek to advance a coordinated Department of Defense-DHS approach to civilian/military supply chain resilience preparedness policy under the National Defense Industrial Strategy's implementation plan. The SCRC is collaborating with the White House and the rest of the Federal Government in the President's Council on Supply Chain Resilience to ensure a whole-of-government response to promote supply chain resilience and protect key systems and infrastructure.

To build our network of allies, the SCRC has begun establishing partnerships with foreign governments. We are working with trusted international governments to develop best practices, identify supply chain risks and shared mitigations, and coordinate exercises to test our capabilities. I am pleased to share that the SCRC will be working with other Executive Branch agencies to partner with our colleagues in Canada to assess port security processes as they relate to supply chains. Together we will conduct a binational interagency tabletop exercise later this year. The exercise will involve a simulated northern border land port disruption of trade and transportation. The exercise will address potential bottlenecks at the U.S.-Canada border and identify best practices to mitigate risks and create a more resilient border.

SCRC & Maritime Infrastructure:

Just weeks after announcing the SCRC, Secretary Mayorkas hosted a roundtable meeting with senior business leaders to introduce the SCRC and how it is leveraging DHS capabilities to identify and mitigate risks with the potential to create major supply chain disruptions. Among the topics raised were the risks posed by PRC-manufactured ship-to-shore cranes.

To better understand and test DHS capabilities to respond to threats to port infrastructure, the SCRC held its inaugural tabletop exercise to understand how the Department might respond to a supply chain disruption caused by a port cyber incident affecting ship-to-shore crane operability. Participants included members from the U.S. Coast Guard (USCG), Cybersecurity and Infrastructure Security Agency (CISA), U.S. Customs and Border Protection (CBP), Federal Emergency Management Agency (FEMA), Transportation Security Administration (TSA), and U.S. Immigration and Customs Enforcement (ICE). The exercise identified key communication areas that are well implemented, but also highlighted the need for holistic coordination planning across the Department. Our next action will be an after-action review that will provide analysis and recommendations informed by the exercise. Moving forward, we are also working to research and map key U.S. maritime infrastructure for homeland security equities. This comprehensive analysis will combine trade import data, DHS critical infrastructure information, and DHS and interagency geospatial data, and will help us to understand the landscape of U.S. maritime infrastructure security.

Concurrently, the SCRC is evaluating the risks to U.S. ports posed by adversarial nation state threats and the potential overreliance on untrustworthy equipment and vendors that are subject to nation-state control and may pose data exploitation, insider threat, and unvetted virtual and physical access risks. The SCRC is closely collaborating with port authorities and operators, other industry stakeholders, and the interagency to conduct this analysis. With this analysis, the SCRC has worked closely with USCG and CISA to verify that our authorities and capabilities are current to keep pace with this emerging threat.

Finally, the SCRC is pleased to expand upon the messages promulgated by President Biden and Secretary Mayorkas in the recent release of the Executive Order on *Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States*, USCG's Maritime Security Directive on cyber risk management actions for PRC-manufactured cranes, USCG's Notice of Proposed Rulemaking on Cybersecurity in the Maritime Transportation System, and the Administration's announcement that PACECO Corp., a subsidiary of Japanese conglomerate Mitsui, is planning to onshore crane production. To amplify these announcements, the SCRC hosted a private sector roundtable with USCG and the Office of Intelligence and Analysis to discuss the threat landscape, highlight the Executive Order's impact on port security, and gather more information from industry representatives about concerns they have.

Foreign Investment Screening:

The United States remains vigilant against the threats to the security of our nation's critical infrastructure that may arise from foreign investments such as investments in our trade and logistics sector, including our maritime ports. In addition to the SCRC's efforts, DHS has played a leading role for the past two decades on the Committee on Foreign Investment in the United States (CFIUS) by identifying and mitigating risks arising from foreign investments in port infrastructure and protecting sensitive trade and logistics data from aggregation and exploitation by foreign adversaries. By law, CFIUS analyzes the facts and circumstances of each foreign investment in port infrastructure within its jurisdiction on a case-by-case basis, following a rigorous risk-based review process. In recent years, DHS has increasingly used its role in CFIUS to lead Committee reviews and mitigation efforts related to foreign investments in U.S. container terminals, and DHS will continue to identify and mitigate other investments in U.S. maritime physical infrastructure that pose national security risks.

Through CFIUS, DHS is also moving to address new and emerging risks in the maritime space. Beyond ports, PRC investments in the global shipping and logistics supply chain permit Beijing to aggregate sensitive supply chain data, which can be exploited to target supply chain vulnerabilities, circumvent U.S. customs, export control, and forced labor laws, and monitor U.S. military logistics. As the U.S.-China Economic and Security Review Commission noted in its 2022 issue brief, *LOGINK: Risks from China's Promotion of a Global Logistics Management Platform*, China aims to monitor and shape the movement of goods around the world, including by accruing dominant market positions in shipping. The PRC increasingly seeks to collect data in foreign markets related to the shipment of goods, exemplified by the PRC Ministry of Transportation's promotion of LOGINK, a unified logistics platform to pool logistics and shipment tracking data. PRC equity investments in freight forwarders, non-vessel operating

common carriers (NVOCCs), and other third-party logistics firms may permit Beijing to aggregate and exploit trade and logistics data. DHS will use the full range of authorities available, including CFIUS, to identify national security risk, take appropriate measures such as mitigation, and – where necessary – recommend divestment to the President to protect national security.

DHS Component Efforts to Protect Maritime Ports:

The Department leverages its wide range of expertise and authorities to protect key transportation infrastructure and advance the resilience of the U.S. supply chain. In addition to USCG, which serves as the co-Sector Risk Management Agency (SRMA) for the maritime subsector and regulator for covered maritime facilities and vessels, other DHS operational Components work diligently every day to facilitate the safe and lawful flow of goods and people upon which our economic security relies.

CBP secures ports of entry throughout the United States, facilitating the lawful flow of people and goods across our borders, and deterring threats from bad actors. CBP has led the way in securing our trade infrastructure with innovative initiatives like the Customs Trade Partnership Against Terrorism. CBP has tailored this program for the maritime port community, developing security standards for marine port authority and terminal operators. CBP leverages a wide range of trade data to target high-risk cargo, enforce our nation's trade laws, protect key infrastructure, and promote supply chain resilience.

TSA plays a key role in securing our nation's transportation systems, including aspects of maritime ports, through enrollment, vetting, and credentialing programs. In partnership with USCG, TSA administers the Transportation Worker Identification Credential (TWIC), which screens workers who access the most secure areas of our maritime ports. Through the TWIC, TSA vets millions of transportation workers including longshoremen, truck drivers, and merchant mariners.

CISA works to manage and reduce risk to our nation's critical infrastructure. CISA takes a unique approach to this mission, partnering closely with critical infrastructure owners and operators and other government agencies to assess risk across the country. CISA works collaboratively with USCG, TSA, other SRMAs, and public and private sector partners to develop risk mitigation solutions for critical infrastructure organizations of all sizes. Port owners and operators can consult a range of CISA cyber and physical security guides and even request one-on-one guidance from CISA through its cadre of local and regional security advisors.

FEMA supports port owners and operators through the Port Security Grant Program in partnership with USCG. This program offers vital funding to protect ports from adversaries, enhance security risk management, improve maritime domain awareness, and implement maritime security mitigation protocols that can help ports prepare for and respond to a range of hazards.

Conclusion:

The Department is dedicated to preparing for, responding to, and mitigating any and all threats to U.S. supply chains. We are deeply committed to our national and economic security missions and ensuring all stakeholders are prepared for the threats of tomorrow. I appreciate this opportunity to testify on this issue, and I look forward to answering your questions.