PORT CYBERSECURITY: THE INSIDIOUS THREAT TO U.S. MARITIME PORTS

HEARING

BEFORE THE

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

FEBRUARY 29, 2024

Serial No. 118–53

Printed for the use of the Committee on Homeland Security

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

57–402 PDF WASHINGTON : 2024

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
DAN BISHOP, North Carolina
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
NICK LALOTA, New York
MIKE EZELL, Mississippi
ANTHONY D'ESPOSITO, New York
LAUREL M. LEE, Florida
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
SHEILA JACKSON LEE, Texas
DONALD M. PAYNE, JR., New Jersey
ERIC SWALWELL, California
J. LUIS CORREA, California
TROY A. CARTER, Louisiana
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
GLENN IVEY, Maryland
DANIEL S. GOLDMAN, New York
ROBERT GARCIA, California
DELIA C. RAMIREZ, Illinois
ROBERT MENENDEZ, New Jersey
THOMAS R. SUOZZI, New York
YVETTE D. CLARKE, New York

STEPHEN SIAO, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY

CARLOS A. GIMENEZ, Florida, *Chairman*

CLAY HIGGINS, Louisiana
NICK LALOTA, New York
LAUREL M. LEE, Florida
MARK E. GREEN, MD, Tennessee *(ex officio)*

SHRI THANEDAR, Michigan, *Ranking Member*
DONALD M. PAYNE, JR., New Jersey
ROBERT GARCIA, California
BENNIE G. THOMPSON, Mississippi *(ex officio)*

VACANCY, *Subcommittee Staff Director*
ALEX MARSTON, *Minority Subcommittee Staff Director*

CONTENTS

PORT CYBERSECURITY: THE INSIDIOUS THREAT TO U.S. MARITIME PORTS

Thursday, February 29, 2024

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON TRANSPORTATION AND
MARITIME SECURITY,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:08 a.m., at Room 310, Cannon House Office Building, Hon. Carlos A. Gimenez [Chairman of the subcommittee] presiding.

Present: Representatives Gimenez, Higgins, Lee, Thanedar, Payne, and Garcia.

Also present: Representatives D'Esposito, Pfluger, and Menendez.

Chairman GIMENEZ. The Homeland Security Subcommittee on Transportation and Maritime Security will come to order. Without objection the Chair may declare the subcommittee in recess at any point. Today's hearing will examine threats to U.S. ports infrastructure, particularly concerning ship-to-shore cranes. Without objection, the gentleman from Texas, Mr. Pluger, the gentleman from New York, Mr. D'Esposito, the gentleman from Mississippi, Mr. Ezell, and the gentleman from New Jersey, Mr. Menendez, are permitted to sit with the subcommittee and ask questions of the witnesses.

I now recognize myself for an opening statement. Today we are here to discuss a matter of national urgency that strikes at the very heart of our Nation's economic vitality and security, the integrity of our maritime infrastructure. This includes port equipment, such as ship-to-shore cranes and other operational technology in wide-spread use at American ports, and that it is manufactured or installed in the People's Republic of China. The proliferation of port equipment and operational technology manufactured or installed by PRC engineers at our Nation's ports introduces significant supply chain vulnerabilities into our maritime transportation system. As a country, we must acknowledge and assess these risks, threats, and vulnerabilities, and decide how to effectively respond.

When I was mayor of Miami Dade County, I witnessed first-hand the critical role that ports lay in our local, national, and global economy. Our ports are not just hubs of commerce, they are gateways to the world. However, our ports are increasingly vulnerable given the evolving threat landscape. We must address this issue with the utmost seriousness. Last week, the Biden administration signed an Executive Order providing the U.S. Coast Guard with

new authorities to respond to potential malicious actors targeting our maritime sector, and particularly those from the PRC. I commend the administration in this initial action, but I know that more must be done.

The ship-to-shore cranes towering over our docks, while instrumental to our port operations, have become a focal point of concern. Most of these cranes are made by CPMC, a PRC state-owned enterprise under the direct control of the CCP. I have witnessed firsthand the destructive power of communist regimes and have no interest in allowing the CCP to conduct industrial and economic espionage in our ports through their cranes.

Last March, Chairman Gallagher of the Select Committee on the CCP and I visited Port Miami to speak directly with port operators and to highlight the legislative efforts we are undertaking to safeguard our ports. This Congress, I introduced the Port Crane Security and Inspection Act. This piece of legislation is a testament to our commitment to ensuring that the backbone of our maritime infrastructure is not compromised. In addition, I have led an ongoing joint investigation with the Select Committee on the CCP to deepen our understanding of the risks at hand. We have learned that these ship-to-shore cranes, which are essential to our maritime operations, could potentially be used as conduits for espionage or as a CCP Trojan horse that threatened to undermine our national security.

The findings are clear. Nearly 80 percent, and I will repeat that, nearly 80 percent of the ship-to-shore cranes in our ports in the United States come from CPMC. This near-monopoly not only presents cybersecurity threats, but also supply chain vulnerabilities that could be exploited by those who wish to inflict damage to our Nation. Monopoly allows for CPMC to compromise U.S.-bound cranes that would cause malfunction or facilitate cyber espionage.

Fortunately, communist China's influence in supply chain extends beyond the state-owned enterprises like CPMC. Third-party companies often create the internal operational components for these ship-to-shore cranes. These include programmable logic controllers, which control many of the ship-to-shore crane systems, as well as crane drives and motors. In most cases, CPMC requires that these companies ship their components to the PRC, where they can be installed by CPMC engineers or technicians.

In the context of our on-going investigation, our committee has explored the role of ABB, a Swiss engineering firm. ABB provides its components directly to CPMC engineers to install on cranes in communist China. I have requested information from ABB's U.S. Country Holding officer about the company's supply chain security practices, as well as other companies with ties to the CCP. Better understanding their practices gives us a broader picture of how their components may be compromised. I was discouraged that ABB had not been as forthcoming as they should have been, particularly when it involves U.S. national security.

Resolving these concerns is crucial for ensuring the security and integrity of the United States maritime infrastructure and protecting against the risks associated with foreign influence and control over critical supply chains. We cannot stand idly by while components of American maritime infrastructure could be weaponized

against us. It is not just about commerce. It is also about national security, about protecting the very fabric of our society from those who seek to unravel it. Going forward, we must take decisive action to secure our ports, to invest in domestic manufacturing of port infrastructure, and to ensure that every ship-to-shore crane, every bolt, every piece of equipment that operates within our borders is safe, secure, and serves the interests of the United States.

[The statement of Chairman Gimenez follows:]

STATEMENT OF CHAIRMAN CARLOS A. GIMENEZ

Today, we are here to discuss a matter of national urgency that strikes at the very heart of our Nation's economic vitality and security: the integrity of our maritime infrastructure. This includes port equipment, such as ship-to-shore cranes and other operational technology, in wide-spread use at American ports, and that is manufactured or installed in the People's Republic of China.

The proliferation of port equipment and operational technology manufactured or installed by PRC engineers at our Nation's ports introduces significant supply chain vulnerabilities into our Maritime Transportation System. As a country, we must acknowledge and assess these risks, threats, and vulnerabilities and decide how to effectively respond.

When I was mayor of Miami-Dade County, I witnessed first-hand the critical role that ports play in our local, national, and global economy. Our ports are not just hubs of commerce, they are gateways to the world.

However, our ports are increasingly vulnerable given the evolving threat landscape. We must address this issue with the utmost seriousness. Last week, the Biden administration signed an Executive Order providing the U.S. Coast Guard with new authorities to respond to potential malicious actors targeting our maritime sector—and particularly those from the PRC. While I commend the administration on this initial action, more must be done.

The ship-to-shore cranes towering over our docks—while instrumental to our port operations—have become a focal point of concern. Most of these cranes are made by ZPMC, a PRC state-owned enterprise under the direct control of the CCP. I have witnessed first-hand the destructive power of communist regimes, and I have no interest in allowing the CCP to conduct industrial and economic espionage in our ports through their cranes.

Last March, Chairman Gallagher of the Select Committee on the CCP and I visited Port Miami to speak directly with port operators and to highlight the legislative efforts we are undertaking to safeguard our ports.

This Congress, I introduced the Port Crane Security and Inspection Act. This piece of legislation is a testament to our commitment to ensuring that the backbone of our maritime infrastructure is not compromised.

In addition, I have led an on-going joint investigation with the Select Committee on the CCP to deepen our understanding of the risks at hand. We have learned that these ship-to-shore cranes, which are essential to our maritime operations, could potentially be used as conduits for espionage, or as a CCP Trojan horse, that threaten to undermine our national security.

The findings are clear: nearly 80 percent of the ship-to-shore cranes in our ports come from ZPMC, and this near-monopoly not only presents cybersecurity threats but also supply chain vulnerabilities that could be exploited by those who wish to inflict damage on our Nation. The monopoly allows for ZPMC to compromise U.S.-bound cranes that could cause malfunction or facilitate cyber espionage.

Unfortunately, Communist China's influence in the supply chain extends beyond state-owned enterprises like ZPMC. Third-party companies often create the internal operational components for these ship-to-shore cranes. These include programmable logic controllers which control many ship-to-shore crane systems, as well as crane drives and motors. In most cases, ZPMC requires that these companies ship their components to the PRC where they can be installed by ZPMC engineers or technicians.

In the context of our on-going investigation, our committees have explored the role of ABB, a Swiss engineering firm. ABB provides its components directly to ZPMC engineers to install on cranes in Communist China.

I have requested information from ABB's U.S. Country Holding Officer about the company's supply chain security practices, as well as other companies with ties to the CCP. Better understanding their practices gives us a broader picture of how their components may be compromised. I am discouraged that ABB has not been

as forthcoming as they should be, particularly when it involves U.S. national security.

Resolving these concerns is crucial for ensuring the security and integrity of the United States' maritime infrastructure and protecting against the risks associated with foreign influence and control over critical supply chains.

We cannot stand idly by while components of American maritime infrastructure could be weaponized against us. It is not just about commerce; it is about national security, about protecting the very fabric of our society from those who seek to unravel it.

Going forward, we must take decisive action to secure our ports, to invest in domestic manufacturing of port infrastructure, and to ensure that every ship-to-shore crane, every bolt, and every piece of equipment that operates within our borders is safe, secure, and serves the interests of the United States.

Chairman GIMENEZ. With that, I will yield back. Now I recognize a Ranking Member, Mr. Thanedar, for his opening statement.

Mr. THANEDAR. Good morning, everybody, and thank you, Chairman Gimenez, for your kindness in accommodating my lateness here. I also thank you for calling today's important and timely hearing. Thank you also to our panel of witnesses for sharing your expertise today.

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 United States 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 Nation's economy. The daily life of Americans everywhere depends upon the ability of government experts, port owners, operators, and their partners in stakeholders to protect ports and rest of the marine transportation system from both physical and cyber attacks.

As ports have become increasingly networked and reliant on computer systems, the importance of instituting strong cybersecurity protections has arisen dramatically. We have already seen the devastating impacts of attacks on ports can have cyber attacks on ports in the United States and overseas have brought the transport of cargo to a standstill and cost hundreds of millions of dollars in economic damage. Thankfully, the Biden administration is taking decisive actions. 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 USC ports, covering a wide range of proven security measures to strengthen our cyber defenses.

Finally, the Coast Guard has 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 Biden administration's comprehensive approach to addressing long-standing cybersecurity threats to critical infrastructure.

Following Colonial Pipeline ransomware attack, the administration committed to raising the cybersecurity baseline and 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 of operators in certain sectors to make security investments in partnership with the Federal Government. These sprints leverage DHS resources and enhance cybersecurity across a wide range of critical areas. To date, these sprints have covered ransomware, the cybersecurity work force, 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 rail to aviation. Last November, the Biden administration announced the creation of Supply Chain Resilience Centers 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 threat, 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 actions 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. I'm hopeful the plan announced by Congressional leaders yesterday will help keep the Government open. A Government shutdown would be devastating to the Coast Guard's operation, including its efforts to implement cybersecurity enhancement. I look forward to hearing more about these critical efforts from our witnesses and, Chairman. I yield back.

[The statement of Ranking Member Thanedar follows:]

STATEMENT OF RANKING MEMBER SHRI THANEDAR

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 United States 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 cyber attacks. 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 cyber attacks on ports can have. Cyber attacks on ports in the United States 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 long-standing 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.

Chairman GIMENEZ. Thank you, to the Ranking Member. Now other Members of the Committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 29, 2024

The Committee on Homeland Security has a long history of conducting oversight of the Department of Homeland Security's efforts to secure critical infrastructure, including maritime ports. As threats have evolved and adversaries have targeted our supply chains and cyber defenses, the Department's mission has grown increasingly complex.

We have seen the impacts of ransomware and other cyber attacks across a range of critical infrastructure sectors, including the maritime sector, both within the United States and internationally. In 2017, for example, a ransomware attack against Danish shipping company A.P. Moller-Maersk led to a shut-down of the Port of Los Angeles' largest cargo terminal along with several others around the world. The attack slowed shipping across the globe for weeks and cost Maersk as much as $300 million.

Just last summer, a ransomware attack caused Japan's busiest shipping port to shut down operations for 2 days. And though ransomware attacks have caused the

most harm to date, we are also aware of the vulnerabilities posed by the decline in U.S. manufacturing over the past several decades and the increased reliance on pieces of critical infrastructure manufactured overseas.

The United States has become heavily reliant on Chinese manufacturing in particular, and China hit an all-time high for its share of total U.S. manufacturing trade under the previous Presidential administration in 2020.

This committee has long studied the vulnerabilities caused by U.S. reliance on Chinese manufacturing across a range of products, including semiconductors, drones, subway cars, and—as we are discussing today—ship-to-shore container cranes used at many U.S. seaports. Addressing these challenges will require steady and consistent dedication and investment over the coming decades, and I am glad to see there is bipartisan commitment to doing so.

Thankfully, the Biden administration has taken unprecedented action to set our Nation on the right path to securing our critical infrastructure and supply chains. Last Congress, President Biden signed into law the Bipartisan Infrastructure Law, the CHIPS and Science Act, and the Inflation Reduction Act, among other legislation. Collectively, these laws represent the most significant investments in American manufacturing and infrastructure in generations.

Under the Biden administration, DHS has also taken action to secure critical infrastructure and supply chains against cyber threats. In March 2021, Secretary of Homeland Security Alejandro Mayorkas outlined a bold vision for raising the cybersecurity baseline across all sectors. At Secretary Mayorkas' direction, DHS carried out a series of 60-day "cybersecurity sprints" on a wide range of topics, leveraging DHS resources and encouraging owners and operators of critical infrastructure to invest in cybersecurity enhancements in partnership with the Government.

Following the ransomware attack against Colonial Pipeline in May 2021, the Transportation Security Administration issued new cybersecurity mandates for pipelines, freight and passenger rail, mass transit, and aviation. Last November, DHS announced the creation of the Supply Chain Resilience Center, which is studying ways to enhance the resiliency of maritime ports as a top priority. And just last week, the Biden administration announced a series of aggressive actions to secure the maritime sector.

President Biden signed an Executive Order to require cyber incident reporting and provide the Coast Guard express authority to act in response to cyber threats. The Coast Guard issued a notice of proposed rulemaking to build on the mandates TSA has issued across transportation modes and require maritime partners to institute similar cybersecurity measures. The Coast Guard also issued a directive to protect ports from the vulnerabilities posed by foreign-manufactured cranes.

Finally, the Biden administration announced a $20 million investment in port infrastructure, using funding from the Bipartisan Infrastructure Law and the Inflation Reduction Act. This investment includes an agreement with the PACECO Corporation to manufacture port cranes within the United States for the first time in more than 30 years. I look forward to learning more about these recently-announced efforts from our witnesses today.

I also look forward to working with my colleagues on both sides of the aisle to secure the funding needed to ensure these actions can be implemented as effectively as possible. The security of U.S. ports is paramount, and I am glad our committee has maintained its focus on these issues.

Chairman GIMENEZ. Again, I am pleased to have a distinguished panel of witnesses before us today on this critical topic. I ask that our witnesses please rise and raise their right hands.

[Witnesses sworn.]

Chairman GIMENEZ. Let the record reflect that the witnesses have answered in the affirmative. Thank you, and please be seated.

I would now like to formally introduce our witnesses. Rear Admiral Derek Trinque serves as director for strategic plans, policy, and logistics for U.S. Transportation Command. Rear Admiral Wayne Arguin serves as the assistant commandant for prevention policy for the U.S. Coast Guard. Rear Admiral John Vann serves as the commander for the U.S. Coast Guard Cyber Command. Ms. Christina Brzozowski serves as the acting assistant secretary for the Trade Economic Security Office of Strategic Policy and Plans for

the Department of Homeland Security. I challenge you to do that in one breath.

I thank each of our distinguished witnesses for being here today. I recognize Rear Admiral Trinque for 5 minutes to summarize his opening statements.

STATEMENT OF REAR ADMIRAL DEREK TRINQUE, DIRECTOR OF STRATEGIC PLANS, POLICY, AND LOGISTICS (J5/J4), UNITED STATES TRANSPORTATION COMMAND (TRANSCOM)

Admiral TRINQUE. Thank you, sir. Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the committee. I'm honored to be here with my colleagues from the United States Coast Guard and Department of Homeland Security to discuss U.S. Transportation Command's key role with strategic seaports. USTRANSCOM is a functional warfighting combatant command, including three component commands, the Air Force's Air Mobility Command, the Navy's Military Sealift Command, and the Army's Surface Deployment and Distribution Command. Together, we provide support to the 10 other U.S. combatant commands, the military services, defense agencies, and other Government organizations. We are an agile and resilient logistics enterprise, which conducts globally integrated mobility operations, leads the broader joint deployment and distribution enterprise, and provides enabling capabilities to project and sustain the joint force in support of national objectives.

With a changing strategic and operational landscape, our logistics and mobility enterprise will play an increasingly critical role in achieving our National defense objectives. On any given day, USTRANSCOM is conducting more than 400 airlift missions, more than 40 air refueling missions, and transporting 10 patients through air evacuation. We have an aircraft taking off and landing every 2 to 3 minutes, over 200 rail cars en route, 30 ships under way, 1,500 freight shipments en route, 20 defense couriers en route, and 1,200 personal vehicle and property shipments en route. To remain successful, USTRANSCOM must be ready to project power today and tomorrow, and we will only achieve this through our partnerships with commercial industry.

Our competitors watch our every move and quickly digest lessons to improve their ability to disrupt, degrade, or deny our capabilities. We synchronize our operations, activities, and investments to balance the enterprise's attention on today's requirements while preparing to meet those of tomorrow. To maximize our role across the spectrum of competition and conflict, we align our campaigning objectives across the primary elements of our warfighting strategy.

Strategic seaports are vital nodes in the Nation's transportation network and play a critical role in the Department of Defense's ability to deploy forces and equipment world-wide. Only 18 of all U.S. commercial seaports are officially designated DoD strategic seaports. These strategic seaports are particularly critical to USTRANSCOM ability to project military power. USTRANSCOM oversees and directs strategic transportation operations executed by Military Sealift Command and Military Surface Deployment and Distribution Command. In this role and under DoD guidance, USTRANSCOM, in coordination with port security stakeholders,

will conduct, arrange, and/or augment other agencies' port assessment activities to identify and remediate vulnerabilities to infrastructure critical to strategic deployment and sustainment missions. In direct coordination with applicable U.S. Coast Guard captains of the port, the results of these assessments are shared with appropriate port security stakeholders while protecting controlled, unclassified information.

The Ports for National Defense program provides the engineering and analytic foundation for the DoD Strategic Seaport program. We work with our partners in the National Ports Readiness Network, including Surface Deployment and Distribution Command, Military Sealift Command, U.S. Northern Command, U.S. Army Forces Command, the U.S. Coast Guard, U.S. Army Corps of Engineers, the Transportation Security Agency, and the Department of Transportation's maritime administration, who also serves as the chair for the NPRN to establish formal coordination and cooperation with the commercial seaports, most important to DoD.

USTRANSCOM is the Department of Defense's single port manager and maintains agreements with each of these commercial ports to support timely access to the facilities needed to conduct a large-scale rapid deployment. Each port, alongside the maritime administration, generates and maintains a port readiness plan. This plan identifies the specific port facilities that would be made available to DoD at time of need. Strategic seaports voluntarily participate in the program. We are grateful for seaport participation as a vital aspect of USTRANSCOM's ability to project power in support of our Nation.

Again, I thank you for the invitation to be a witness at this hearing, and I look forward to answering your questions.

[The prepared statement of Admiral Trinque follows:]

PREPARED STATEMENT OF REAR ADMIRAL DEREK TRINQUE

29 FEBRUARY 2024

WHO WE ARE—OUR MISSION

U.S. Transportation Command's (USTRANSCOM) enduring purpose is to project and sustain combat power whenever and wherever our Nation chooses. As 1 of 11 combatant commands, our warfighting team is a diverse force, comprised of 3 component commands, 1 subordinate command, our allies, and our interagency and commercial partners—all of which constitutes the broader Joint Deployment and Distribution Enterprise (JDDE). Within the ever-changing strategic and operational landscape, our logistics and mobility enterprise continue to play an integral role in assuring our Nation's defense as well as to provide our national leadership strategic advantage. We must ensure the Joint Force can defend the Nation, take care of our people, and succeed through teamwork. To deter and win, the 2022 National Defense Strategy (NDS) directs the Future Joint Force to be lethal, resilient, sustainable, survivable, agile, and responsive.

The entire JDDE works together to move the right capabilities to the right place, at the right time. Our assigned Unified Command Plan (UCP) responsibilities are executed through three component commands (U.S. Army's Military Surface Deployment and Distribution Command, U.S. Navy's Military Sealift Command, and U.S. Air Force's Air Mobility Command), and one major subordinate command (Joint Enabling Capabilities Command [JECC]). Our key mobility mission areas include sealift, strategic seaports, air refueling, airlift, aeromedical evacuation, domestic rail, and motor and barge freight. The JDDE operates as a Total Force, harnessing the unique skills of Active Duty, Reserve, National Guard, Merchant Marine, and Civilian teammates who are vital to our ability to bolster warfighting readiness.

The Department of Defense's (DoD) ability to project military forces is inextricably linked to commercial industry. Our industry partners provide critical transportation

capacity and global networks to meet day-to-day and wartime requirements. USTRANSCOM also partners with other U.S. Government departments and agencies, such as the U.S. Department of State and U.S. Department of Transportation (DoT), especially the Maritime Administration (MARAD) as it operates and maintains the Government-owned sealift fleet and oversees the administration of the Strategic Seaport Program. Within DoT we also interconnect with the Federal Highway, Federal Motor Carrier Safety, and Federal Railroad Administrations regarding DoD transportation requirements within CONUS, including rapid equipment movement needs from "fort to the port" on our national highway and railroad networks. In addition to DoT, we partner with the Defense Logistics Agency (DLA), the General Services Administration, and other key logistics partners who provide the funding for deployment and distribution operations as well as the Department of Homeland Security (DHS), the U.S. Coast Guard (USCG), the Transportation Security Agency, and many more. Both individually as well as collectively, this entire collective group of partners support as well as guide our efforts and are also customers of the Defense Transportation System.

With our partners, USTRANSCOM works hard to develop the most robust transportation network possible, both for current and future operations. Because our networks are vulnerable to a wide range of threats, from climate change to nation-state cyber attacks, USTRANSCOM plans, operates, and routinely exercises so that our forces can operate through disruption. This includes operating with partners in a cyber-degraded or -denied environment and quickly and creatively rerouting critical supplies to support our warfighters. I will address some of our flagship efforts today.

STRATEGIC SEAPORT PROGRAM

To successfully execute our deployment mission, USTRANSCOM relies on a collection of both DoD and commercially-owned U.S. strategic seaports managed through the Strategic Seaport Program. Strategic seaports are vital nodes in the Nation's transportation network and play a critical role in DoD's ability to deploy forces and equipment world-wide—6 military seaports and 18 U.S. commercial seaports are officially designated as primary DoD strategic seaports with an additional 1 military and 13 U.S. commercial seaports identified as alternate seaports.

The basis for the program can be found in various Government publications, including Executive Order 12656 regarding the assignment of emergency preparedness responsibilities. These publications direct Federal departments to identify facilities and resources, both Government and private, essential to the national defense and mobilization readiness; assess the vulnerabilities and develop strategies, plans and programs to provide for the security of such facilities and resources; and to avoid or minimize disruptions of essential services during any national security emergency. The primary purpose of the Strategic Seaport Program is to ensure DoD has access to sufficient seaport capacity to meet the Nation's objectives.

STRATEGIC SEAPORTS

Within the UCP, USTRANSCOM is identified as the DoD Single Port Manager. The Military Surface Deployment and Distribution Command (SDDC), as the surface transportation component to USTRANSCOM, executes the Strategic Seaport Program for the DoD. Strategic seaports are formally designated by the Commanding General, SDDC, based on anticipated deployment requirements related to plausible major contingencies, emergencies or disasters, and war. Although participation in the Strategic Seaport Program is voluntary, the strategic seaports accept specific planning and reporting responsibilities.

NATIONAL PORT READINESS NETWORK

Once designated, the strategic seaports are administratively managed through the National Port Readiness Network (NPRN). The NPRN is made up of 9 Government agencies including USTRANSCOM, SDDC, Military Sealift Command (MSC), U.S. Northern Command, U.S. Forces Command, U.S. Coast Guard (USCG), U.S. Army Corps of Engineers, Transportation Security Agency, and MARAD who Chairs the NPRN. The NPRN provides coordination and cooperation to support the safe and secure movement of military forces through the strategic seaports. A Memorandum of Understanding (MOU) outlines each of the 9 agencies' roles, responsibilities, and authorities to facilitate planning and support port readiness.

Port Readiness Plans

Each designated primary strategic seaport has a Port Readiness Plan (PRP) which identifies the specific port facilities and berths that would be made available to DoD within 48 hours of issuance of a rated order contract. These port facilities include

berths, open and covered staging areas, rail spurs, and marshaling yards which can readily accommodate the trans-load of substantial numbers of DoD's rolling stock and containers within anticipated short time lines. MARAD serves as the primary interface with the commercial strategic seaports to establish and maintain the PRPs.

Port Readiness Committees

Chaired by the USCG Captain of the Port (COTP), the Port Readiness Committee (PRC) is convened biennially to facilitate training and periodic exercises to ensure the readiness of the port to support military operations. The PRC is comprised of local port or port area representatives that coordinate, evaluate, and test military out load plans, force protection/military out load security and facilitate out loads.

Readiness Reporting

The strategic seaports formally report to MARAD quarterly on their ability to make PRP facilities available to support DoD's needs. Informal, off-cycle reporting is also completed as events warrant. Additionally, MARAD conducts an annual Enhanced Port Readiness Assessment on each strategic port, with the assistance of the other members, to ensure the PRC has a current understanding of the port's ability to support military operations. These assessments cover the availability of facilities and labor, port access, port security, and other factors that may interfere with deployment.

PORTS FOR NATIONAL DEFENSE PROGRAM

The director of SDDC's Transportation Engineering Agency is designated as the special assistant for transportation engineering to provide executive-level representation for DoD on all transportation engineering matters related to the National Defense Programs (Ports, Highways, Railroads). These programs ensure DoD can readily access and utilize the Nation's civil sector infrastructure to support major force deployments by assessing and monitoring the sufficiency and viability of all elements of the related infrastructure. The Ports for National Defense Program (PND) provides the engineering/analytical foundation for the DoD Strategic Seaport Program pursuant to Executive Order 12656 and in accordance with the authority in the Defense Production Act of 1950 (50 U.S.C. Section 4502, et seq.) by managing the identification and assessments of strategic seaports.

The PND Office views strategic seaport capacities from an aggregated coastal perspective (East, Gulf, West, Alaskan), and in the Pacific. Each coast currently has the aggregate capacity necessary to respond to plausible deployment requirements while also accounting for normal delays (e.g., weather, transportation, etc.) and the potential loss of one or more strategic seaports to manmade events or natural disasters. The criteria PND uses to support the designation of a strategic seaport extends beyond port infrastructure and throughput capability. Proximity to origins (primarily Army Power Projection Platforms) and the capabilities of the transportation networks connecting these origins to the ports are also considered.

Port Look Studies

Beginning in 2008 with the publication of the original "Port Look Study," DoD has completed multiple reviews/assessments of the sufficiency of the strategic seaports in meeting DoD needs. Many of these reviews/assessments were Congressionally-directed via National Defense Authorization Act (NDAA) language or were the result of Government Accountability Office audit recommendations; however, some were self-imposed in keeping with the tenets of the Strategic Seaport Program.

To evaluate physical conditions at the strategic seaports, the PND Office completed the "Assessment and Report on Strategic Seaports" as directed by Section 3515 of the 2020 NDAA (Public Law 116–92). USTRANSCOM submitted this report to Congress in July 2020. This study found that while many of the ports assessed were found to have varying degrees of structural deficiencies associated with PRP facilities, none of these deficiencies were assessed to have significant impacts on near-term deployment operations.

The PND Office also recently completed the "Port Look 2021" study. This study assessed throughput capabilities at current strategic and alternate seaports, accounted for threats that could have an impact on deployment operations (including cyber), assessed sufficiency of existing strategic seaports to meet expected deployment requirements and made recommendations to address capability gaps. The Port Look 2021 study recommended the designation of an additional strategic seaport on the U.S. West Coast to ensure the strategic seaports on that coast can overcome normal delays and the loss of a port due to manmade events or natural disasters. In

response to that recommendation, the commercial Port of Everett, Washington, was formally designated a strategic seaport in September 2021.

INTERAGENCY SECURITY OF THE STRATEGIC SEAPORTS

While the Coast Guard is designated by the Secretary of Homeland Security as the lead DHS agency for maritime security, seaport security is a shared responsibility among private ownership, civil authorities, DoD, and other Federal agencies. For example, owners, operators, masters, and agents of vessels or owners and/or operators of waterfront facilities have the primary responsibility for the protection of their vessels or waterfront facilities. Military unit commanders are responsible for the physical security of all equipment and resources under their command. Federal, State, and local law enforcement agencies provide civil support, to include preventing the escalation of lawful protest activity and ensuring continuity of port operations when operations are potentially threatened by labor actions or other forms of civil disturbance.

USCG and the Department of Homeland Security have overall responsibility and enforcement authority for the safety, protection, and security of vessels, harbors, waterfront facilities, and maritime critical infrastructures and key resources that are carried out by the USCG Captain of the Port. As mentioned earlier, the COTP is the chair of respective NPRN PRCs, and assists in further coordinating interagency efforts regarding port readiness issues.

The Navy (delegated to the Naval Component Commanders) is responsible for force protection of military sealift assets. MSC, the naval component to USTRANSCOM, its Area Commands, and/or the local MSC Office coordinates for appropriate security support at commercial ports with the USCG COTP and the SDDC Brigade/Battalion Commander.

SDDC Transportation Brigade/Battalion security personnel coordinate with the appropriate port security/law enforcement authority where DoD operations are being conducted. SDDC conducts threat assessments based on Force Protection Conditions, Maritime Security (MARSEC) level, applicable National Terrorism Advisory System alerts and available intelligence and will coordinate with the COTP and Port Support Activity to ensure appropriate balanced landside and waterside safety and security measures around deployment activities.

MISSION IMPACTS—RESILIENCY

In general, if strategic seaports fail to maintain viability and availability of the facilities outlined in their PRPs, the DoD could exercise several options to support deployment and the DoD response to national emergencies. Such options include increasing or changing PRP facilities at existing strategic seaports, for example negotiating for more or different marshalling areas, number of berths, staging area locations/square footage, etc. DoD could also consider designating different or additional strategic seaports. Finally, as previously explained, the Strategic Seaport Program is intentionally designed to carry excess capacity to mitigate lost seaport access due to exogenous events.

Mission Assurance and Risk Management

The Secretary of Defense's recently-issued "Homeland Defense Policy Guidance 2023" which supports implementation of the 2022 National Defense Strategy's highest priority, defending the homeland, paced to the growing multi-domain threat posed by China.

Consistent with the Homeland Defense Policy Guidance, USTRANSCOM manages risk to Defense Critical Infrastructure (DCI) through the Mission Assurance (MA) Construct which is a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DoD mission-essential functions in any operating environment or condition. Central to this construct is the Secretary of Defense's signed Mission Assurance Strategy with the message that in today's global risk environment, strategic planning for core defense missions must account for a wide variety of man-made and naturally-occurring threats and hazards and their resultant vulnerabilities. The Mission Assurance Strategy provides the Department with a Mission Assurance-centric framework focused on ensuring resiliency for the capabilities and assets supporting our core missions.

The MA Construct outlines the process to identify the most important capabilities and assets needed for the Department to carry out its missions. These capabilities face multiple threats such as natural disasters, foreign intelligence collection, and kinetic and cyber threats. To successfully address these threats and hazards re-

quires the collective expertise, responsibilities, and authorities from multiple organizations within the DoD and external to the DoD.

Through the MA Construct, we work across DoD to identify, analyze, assess, and monitor DCI strategic-level risks to global mobility operations and mission execution. This strategic level of risk management effort addresses the protection and resiliency of DCI identified as critical to Operation Plan execution. Commercial, privately-owned and -operated infrastructure, and non-DoD publicly-owned infrastructure are considered DCI to include seaports if they support a DoD mission.

CONCLUSION

In conclusion, strategic seaports are vital nodes in the Nation's transportation network and play a critical role in DoD's ability to deploy forces and equipment world-wide. We have designated 18 commercial strategic seaports and 6 military strategic seaports, 13 alternate commercial seaports, and 1 alternate military seaport. Each designated strategic seaport has a mutually-agreed-upon Port Readiness Plan (PRP) which identifies both DoD's and the port's needs, expectations, and time line requirements. Although participation in the Strategic Seaport Program is voluntary, each designated strategic seaports accepts specific planning and reporting responsibilities.

The coordination between USTRANSCOM and the Department of Homeland Security and the U.S. Coast Guard concerning the security of strategic seaports is multi-fold. Such coordination includes roles and responsibilities as identified within the NPRN nine-member interagency MOU. Each designated strategic seaport has an established Port Readiness Committee which is chaired by the USCG Captain of the Port. The committee is comprised of local port or port area representatives (both civilian and military) that coordinate, evaluate, and test military out load plans, force protection/military out load security and facilitate out loads. Through the Mission Assurance Construct, USTRANSCOM also synchronizes inputs and coordinates discussions across USTRANSCOM staff directorates, component commands, DoT, DHS, as well as other relevant mission partners to include Federal Law Enforcement and Counterintelligence Communities directly supporting commercial ports.

To ensure the Joint Force's ability to deploy via our seaports, our Ports for National Defense Office has rigorously reviewed, analyzed, and compared DoD's requirements to port locations, viabilities, and capabilities. The Strategic Seaport Program is intentionally designed to carry excess capacity in order to mitigate potential lost seaport access. Each U.S. coast has the aggregate capacity necessary to respond to deployment requirements while also accounting for normal delays (e.g., weather, transportation, etc.) and the potential loss of one or more strategic seaports to man-made events or natural disasters.

All in all, to remain successful, USTRANSCOM must be ready to project power today and tomorrow, and we will only achieve this together. The contested nature of logistics highlights that our actions to improve mobility capabilities and to modernize the JDDE, must continue in order for the DoD to maintain advantages and deliver on our National security requirements.

Powered by dedicated men and women, USTRANSCOM underwrites the lethality of the Joint Force, advances American interests around the globe, provides our Nation's leaders with strategic flexibility, and creates multiple dilemmas for our adversaries. I thank Congress for your continued support to the men, women, and mission of USTRANSCOM.

Chairman GIMENEZ. Thank you, Rear Admiral Trinque. I recognize Rear Admiral Arguin for 5 minutes to summarize his opening statement.

STATEMENT OF REAR ADMIRAL WAYNE R. ARGUIN JR., ASSISTANT COMMANDANT FOR PREVENTION POLICY, UNITED STATES COAST GUARD

Admiral ARGUIN. Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee. I'm honored to be here today to discuss the United States Coast Guard's efforts to protect the marine transportation system. I ask that my written testimony be entered into the record.

Chairman GIMENEZ. Without objection.

Admiral ARGUIN. Our National security and economic prosperity are inextricably linked to a safe and efficient marine transportation system, or MTS. The vast system of ports and waterways that make up the MTS supports $5.4 trillion of annual economic activity, accounts for the employment of more than 30 million Americans, and enables critical sealift capabilities, allowing our armed forces to project power around the globe. The connectedness and increasing complexity of the MTS brings new vulnerabilities and threats, including the cyber domain.

In response to dynamic threats, the United States Coast Guard has taken decisive action in our maritime critical infrastructure to harden and build resilience against cyber attacks. Just last week, the President signed an Executive Order which further enables our port security efforts by explicitly addressing cyber threats. It empowers the Coast Guard to prescribe conditions and restrictions for the safety of waterfront facilities and vessels in port and includes reporting requirements for actual and threatened cyber incidents. With this authority, the Coast Guard issued a directive requiring specific risk management actions for all owners and operators of cranes manufactured by the People's Republic of China. While the specific requirements are deemed sensitive security information and cannot be shared publicly, our captains of the port around the country are working directly with crane owners to ensure compliance.

Last week, the Coast Guard also released a proposed rulemaking to set baseline cybersecurity requirements for vessels, facilities, and outer continental shelf facilities. The service stresses the need for public participation in the proposed rulemaking. The diversity of the maritime industry and the dynamic nature of the cyber threat make public comment critical. While the Coast Guard is focused on implementing the major efforts initiated last week, work is far from done. The MTS is indeed a system where an attack on one segment has a potential to affect others. This demands collaboration across Government and industry to ensure that a unified and coordinated response to cyber challenges in the maritime domain. Like all other risks to the MTS, cyber risk is a shared responsibility.

As such, the Coast Guard will continue its work across all levels of government and engage with industry to assess security vulnerabilities, determine risk, and deploy mitigation strategies. This layered approach from the local to international level is critical to the size, diversity, and interconnectedness of the MTS. As the proven prevention and response framework is applied to prevent and minimize disruptions to the MTS and ports around the country, I'm grateful for the support of this committee to ensure the Coast Guard has the authorities and the resources needed to stay ahead.

I look forward to your questions on the vital work the Coast Guard does every day to safeguard America's ports. Thank you for the opportunity to appear before you today and for your continued support of the United States Coast Guard.

[The joint prepared statement of Admiral Arguin and Admiral Vann follows:]

JOINT PREPARED STATEMENT OF WAYNE R. ARGUIN AND JOHN C. VANN

29 FEB 2024

INTRODUCTION

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee. We are honored to be here today to discuss a top priority for the U.S. Coast Guard: protecting the Marine Transportation System (MTS). At all times, the U.S. Coast Guard is a military service and branch of the U.S. Armed Forces, a Federal law enforcement agency, a regulatory body, a co-Sector Risk Management Agency, a first responder, and an element of the U.S. intelligence community (IC). The service is uniquely positioned to ensure the safety, security, and stewardship of the maritime domain.

Since the early days of the Revenue Cutter Service, the service has protected our Nation's waters, harbors, and ports. While much has changed over the centuries—with our missions expanding from sea, air, and land into cyber space—our ethos and operational doctrine remain steadfast. Regardless of the threat, we leverage the full set of our authorities; the ingenuity and leadership of our workforce; and the breadth of our military, law enforcement, and civil partnerships to protect the Nation, its waterways, and all who operate on them.

THE CRITICALITY OF THE MARINE TRANSPORTATION SYSTEM

Our national security and economic prosperity are inextricably linked to a safe and efficient MTS. It is difficult to overstate the complexity of the MTS and its consequence to the Nation. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. However, it is more than ports and waterways. It is cargo and cruise ships, passenger ferries, waterfront terminals, offshore facilities, buoys and beacons, bridges, and more. The MTS supports $5.4 trillion of economic activity each year and supports the employment of more than 30 million Americans.

It supports critical national security sealift capabilities, enabling U.S. Armed Forces to project power around the globe. The U.S. Coast Guard remains laser-focused on the safety and security of this system as an economic engine and strategic imperative.

PORT SECURITY—A SHARED RESPONSIBILITY AND LAYERED APPROACH

The U.S. Coast Guard is the Nation's lead Federal agency for safeguarding the MTS. The service applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces. U.S. Coast Guard authorities and capabilities cut across threat vectors, allowing operational commanders to quickly evaluate risks, apply resources, and lead a coordinated and effective response.

The U.S. Coast Guard works across multiple levels of government and industry to assess security vulnerabilities, determine risk, and develop mitigation strategies. This layered approach—from the local to the international level—is critical due to the size and interconnectedness of the MTS.

LOCALLY: VESSEL AND FACILITY SECURITY

Security in U.S. ports and waterways starts with individual vessels, port facilities, and outer continental shelf facilities. The Maritime Transportation Security Act (MTSA) and its implementing regulations place specific requirements on regulated entities to conduct security assessments, analyze the results, and incorporate their findings in U.S. Coast Guard-approved security plans.

These plans set baseline requirements that regulated U.S. vessels and facilities must follow to protect the MTS, including addressing access control, computer systems and networks, restricted area monitoring, communication, security systems, cargo handling, delivery of stores, personnel training, and drills and exercises. U.S. Coast Guard inspectors verify compliance with these plans during scheduled and unannounced inspections throughout a given year. Additionally, the Coast Guard released a proposed rulemaking leveraging the applicability of the MTSA regulations to further raise cybersecurity standards for vessels, facilities, and Outer Continental Shelf facilities. For foreign-flagged vessels, the approach to security is very similar to that of MTSA-regulated domestic vessels. Per the International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code, each foreign vessel must conduct a Ship Security Assessment that identifies: key shipboard operations that are important to protect; possible threats to key shipboard oper-

ations and likelihood of their occurrence; existing security measures and procedures; and potential weaknesses, including human factors, in security policies and procedures. This assessment then leads to the development of a Ship Security Plan, which must be approved by the ship's Flag Administration prior to a vessel being certificated as compliant with the ISPS Code. This certification is verified by the U.S. Coast Guard during regular compliance examinations when the vessel arrives in a U.S. port.

REGIONALLY: AREA MARITIME SECURITY COORDINATION

At the regional level, Area Maritime Security Committees (AMSC) are required by MTSA and its implementing regulations to serve an essential coordinating function during normal operations and emergency response. Comprised of Government and maritime industry leaders, an AMSC serves as the primary regional body to jointly share threat information, evaluate risks, and coordinate risk mitigation activities. As the Federal Maritime Security Coordinator (FMSC), U.S. Coast Guard Captains of the Port (COTP) direct their regional AMSC's activities.

AMSC input is vital to the development and continuous review of the Area Maritime Security (AMS) Assessment and Area Maritime Security Plan (AMSP). The AMS Assessment must include the critical MTS infrastructure and operations in the port; a threat assessment that identifies and evaluates each potential threat; consequence and vulnerability assessments; and a determination of the required security measures for the three Maritime Security levels.

These AMS assessments then lead to the collaborative development of AMSPs to ensure Government and industry security measures are coordinated to deter, detect, disrupt, respond to, and recover from a threatened or actual Transportation Security Incident.

The U.S. Coast Guard COTP and AMSCs are also required by regulations to conduct or participate in an exercise once each calendar year to collectively assess the effectiveness of the AMSP in today's dynamic operating environment.

NATIONALLY: INTERAGENCY COLLABORATION

The U.S. Coast Guard functions on behalf of the Department of Homeland Security as the co-Sector Risk Management Agency (SRMA) for the Maritime Transportation Subsector along with the Department of Transportation. As an SRMA, the U.S. Coast Guard is responsible for coordinating risk management efforts with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders.

CISA is a key partner whose technical expertise supports the U.S. Coast Guard's ability to leverage our authorities and experience as the regulator and SRMA of the MTS. CISA integrates a whole-of-Government response, analyzes broader immediate and long-term impacts, and facilitates information sharing across transportation sectors. Our relationship with CISA is strong and will continue to mature.

As an element of the IC, the U.S. Coast Guard possesses unique authorities, and has opportunity and capability to collect, analyze, and share information from domestic, international, and non-government stakeholders which operate throughout the MTS. This ability allows the U.S. Coast Guard to gain a collective understanding of threats and vulnerabilities facing the maritime domain, including physical security and cybersecurity.

Our enduring relationship with the Department of Defense (DoD) is also crucial to safeguarding the MTS. In many cases, DoD's ability to surge forces from domestic to allied seaports depends on the same commercial maritime infrastructure as the MTS. The relationship between the U.S. Coast Guard and DoD ensures the Nation's surge capability and lines of communication will be secure and available during times of crisis. By sharing threat intelligence, developing interoperable capabilities, and leveraging DoD's expertise, the U.S. Coast Guard enables national security sealift capabilities and jointly supports our Nation's ability to project power around the globe.

The U.S. Coast Guard also supports the Federal Emergency Management Agency (FEMA) in the Port Security Grant Program (PSGP) by providing subject-matter expertise in maritime security. The PSGP is designed to support and protect critical port infrastructure from terrorism. FEMA is responsible for the administration and management of the program, which has distributed more than $3.8 billion to MTS stakeholders since the program's inception in 2002.

INTERNATIONALLY: INTERNATIONAL PORT SECURITY PROGRAM

U.S. Coast Guard efforts to secure the MTS also extend overseas. By leveraging international partnerships, including through the U.S. Coast Guard International

Port Security (IPS) program, the U.S. Coast Guard conducts in-country foreign port assessments to assess compliance with the ISPS Code and the effectiveness of security and anti-terrorism measures in foreign ports. In addition, the IPS program conducts capacity-building engagements to assist foreign ports in implementing effective anti-terrorism measures, where possible.

If the U.S. Coast Guard finds that a country's ports do not have effective security and anti-terrorism measures, the service may impose additional security measures called Conditions of Entry (COE) on vessels arriving to the United States from those ports and may deny entry into the United States to any vessel that does not meet such conditions. Verification that a vessel took additional security measures when it was in foreign ports that lacked effective anti-terrorism measures may be required before the vessel is permitted to enter the United States.

THE GROWING CYBER RISKS

Cyber attacks can pose a significant threat to the economic prosperity and security of the MTS for which whole-of-Government efforts are required. The MTS's complex, interconnected network of information, sensors, and infrastructure continually evolves to promote the efficient transport of goods and services around the world. The information technology and operational technology networks vital to increasing the efficiency and transparency of the MTS also create complicated interdependencies, vulnerabilities, and risks.

The size, complexity, and importance of the MTS make it an attractive cyber target. Terrorists, criminals, activists, adversary nation-states and state-sponsored actors may view a significant MTS disruption as favorable to their interests. Potential malicious actors and their increasing levels of sophistication present substantial challenges to Government agencies and stakeholders focused on protecting the MTS from constantly-evolving cyber threats.

Cyber vulnerabilities pose a risk to the vast networks and system of the MTS. Cyber attacks, such as ransomware attacks, can have devastating impacts on the operations of maritime critical infrastructure. A successful cyber attack could disrupt global supply chains and impose unrecoverable losses to port operations, electronically stored information, and national economic activity. The increased use of automated systems in shipping, offshore platforms, and port and cargo facilities creates enormous efficiencies, but also introduces additional attack vectors for malicious cyber actors. Growing reliance on cyber-physical systems and technologies requires a comprehensive approach by all MTS stakeholders to manage cyber risks and ensure the safety and security of the MTS.

Last week, the President signed an Executive Order which further enables our port security efforts by explicitly addressing cyber threats. It empowers the Coast Guard to prescribe conditions and restrictions for the safety of waterfront facilities and vessels in port and includes reporting requirements for actual or threatened cyber incidents. With this authority, the Coast Guard issued a directive requiring specific cyber risk management actions for all owners or operators of cranes manufactured by companies from the People's Republic of China. Our Captains of the Port around the country are working directly with crane owners and operators to ensure compliance and further mitigate the threats posed by these cranes.

THE U.S. COAST GUARD'S APPROACH

In support of the whole-of-Government effort, the U.S. Coast Guard applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces.

Prevention

The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all prevention missions, including port security. It begins with establishing expectations in the MTS. Regulations and standards provide a set of baseline requirements and are critical to establishing effective and consistent governance regimes. With effective standards in place, vessel and facility inspectors verify systematic compliance activities to ensure the governance regime is working. This part of the system is vital in identifying and correcting potential risks before they advance further and negatively impact the MTS. Effective assessment is paramount to continuous improvement. It provides process feedback and facilitates the identification of system failures so that corrective actions can be taken to improve standards and compliance activities.

In addition to vessel and facility inspectors, the U.S. Coast Guard also has Port Security Specialists and MTS Cybersecurity Specialists in each Captain of the Port Zone. These dedicated staffs build and maintain port-level security-related relation-

ships, facilitate information sharing across industry and Government, advise U.S. Coast Guard and Unified Command decision makers, and plan security exercises.

Response

The U.S. Coast Guard has a proven, scalable response framework that can be tailored for all hazards. Whether a cyber or physical security incident, our operational commanders immediately assess the risk, consider their authorities, and deploy assets or issue operational controls to mitigate risks. Depending on the incident's size and severity, commanders set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response.

For complex responses, the U.S. Coast Guard maintains deployable teams with specialized capabilities that can support operational commanders across a spectrum of needs and domains. These teams include specially-trained law enforcement teams that can bolster physical security, and pollution response teams that can address significant oil spills or hazardous material releases. In addition, the U.S. Coast Guard has established three Cyber Protection Teams as commands under U.S. Coast Guard Cyber Command. These units assist Captains of the Port with measuring cyber risk and are poised to deploy in support of time-critical or nationally significant cyber activities.

FUTURE FOCUS

Given today's dynamic operational environment, the U.S. Coast Guard is ever vigilant and on watch to identify emerging threats, evaluate associated risk, and apply authorities and capabilities to protect the MTS. While the U.S. Coast Guard has a proven prevention and response framework that has been honed over many years, the service is dedicated to continually assessing and enhancing the way we execute both enduring and emerging missions. The U.S. Coast Guard's commitment is to continue to lead with the same level of professionalism, efficiency, and effectiveness that the public has come to expect.

Thank you for the opportunity to testify today and thank you for your continued support of the U.S. Coast Guard. We look forward to answering your questions.

Chairman GIMENEZ. Thank you, Rear Admirable Arguin. I now recognize Rear Admiral Vann for 5 minutes to summarize his opening statement.

STATEMENT OF REAR ADMIRAL JOHN VANN, COAST GUARD CYBER COMMAND, UNITED STATES COAST GUARD

Admiral VANN. Good morning, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee. I'm honored to be here today to discuss the protection, defense, and resiliency of the marine transportation system, the MTS from today's cyber threats. I ask that my written testimony be entered into the record.

Chairman GIMENEZ. Without objection.

Admiral VANN. The Coast Guard is committed to addressing cybersecurity risks and responding to cyber incidents in the marine environment to ensure our Nation's economic and national security. The size, interdependence, complexity, and criticality of the MTS makes it a prime target for criminals, activists, terrorists, State-sponsored actors, and adversarial nation-states. The diversity of potential malicious actors and their increasing levels of sophistication presents substantial challenges to stakeholders and government agencies focused on protecting the MTS from these evolving cyber threats.

The threat of disruptive cyber effects to our critical infrastructure, specifically to the MTS, require us to be vigilant, proactive, collaborative, and resourceful. Cyber intrusions and attacks, such as ransomware attacks, have a devastating impact on transportation critical infrastructure. A successful cyber attack could im-

pose unrecoverable losses to port operations and electronically-stored information, hampering national economic activity, and disrupting global supply chains. The increased use of automated systems in shipping, offshore platforms, and port and cargo facilities creates enormous efficiencies and introduces additional attack vectors for malicious cyber actors. This growing reliance on cyber physical systems and operational technologies requires a comprehensive approach by all stakeholders to manage cyber risks and ensure safety and security of the MTS.

With the support of Congress, the Coast Guard has invested in growing and maturing Coast Guard cyber command to assess, identify, and respond to cyber risks and threats. CG Cyber currently has two cyber protection teams, or CPTs, with a third CPT expected to reach full operational capability later this summer. Using Coast Guard authorities, the CPTs partner with local captains of the port and industry to address cybersecurity risks in the MTS. In fact, a Coast Guard CPT was the first Federal cyber response team in 2021 to identify probable port network intrusion by a People's Republic of China actor known as Volt Typhoon. Our ability to share information and critical vulnerabilities with the Cybersecurity and Infrastructure Security Agency, CISA, and law enforcement partners enabled a timely response and rapid mitigation of risks with that port partner.

CG Cyber's Maritime Cyber Readiness branch, subject-matter experts in cybersecurity and marine safety, regularly engages with industry to improve cyber literacy and support Coast Guard captains of the port in measuring cyber risk. We will soon release the third annual cyber trends and insights in the Marine Environment Report, which provides key insights into trends to aid industry and other stakeholders to identify and address current and emerging cyber risks.

Through consistent work and collaboration with other departments, agencies, and industry, CG Cyber shares critical vulnerability information mitigation strategies, and threat intelligence. Our CPTs regularly deploy with Department of Defense and CISA teams to provide maritime and operational technology subject-matter expertise around the globe. We are better and more resilient because we exercise and execute operations together.

I look forward to continuing this conversation and appreciate the opportunity to answer your questions. Thank you.

Chairman GIMENEZ. Thank you, Rear Admiral Vann. I now recognize Ms. Brzozowski for 5 minutes to summarize her opening statements.

STATEMENT OF CHRISTA BRZOZOWSKI, ASSISTANT SECRETARY FOR TRADE AND ECONOMIC SECURITY, DEPARTMENT OF HOMELAND SECURITY

Ms. BRZOZOWSKI. Good morning, Chairman, Ranking Member, and distinguished Members of the subcommittee. Thank you for the opportunity to discuss the Department of Homeland Security's role in securing maritime infrastructure and bolstering supply chain resilience. The Department is deeply committed to preventing and countering all threats to our national and economic security, in-

cluding cyber attacks and other disruptions that could impact the efficient movement of goods through our Nation's seaports.

To advance this mission, DHS has a wide range of expertise and authorities, including protecting cyber spaces, securing critical infrastructure, facilitating lawful trade and travel, and preparing for and responding to disasters. Alongside the U.S. Coast Guard, DHS employees from the U.S. Customs and Border Protection, the Cybersecurity and Infrastructure Security Agency, the Federal Emergency Management Agency, the Transportation Security Administration, and others, work diligently to protect our seaports. They also work to protect the broader maritime transportation system and other critical infrastructures and address and mitigate against all hazards threatening our security.

At DHS, we are incredibly vigilant and committed to making maritime ports and other critical infrastructures and supply chains as secure as we can. But we live in a world of constantly-evolving threats. We know that adversaries are constantly probing and developing new tactics and that supply chains are vulnerable to a wide range of shocks and disruptions. That's why DHS operational components are continuously monitoring for new risks, providing key services to the private sector, and ensuring that they also recognize and manage these risks as both core business risks and as fundamental to national and economic security.

That's also why we established a new Supply Chain Resilience Center within the Department. The new center serves to coordinate the Department's supply chain efforts and work with partners and allies to research and assess potential threats and plan how we can bolster resilience throughout the U.S. supply chain. The DHS Supply Chain Resilience Center supported the development of the Executive Order on amending regulations relating to the safeguarding of vessels, harbors, ports, and waterfront facilities, and the Coast Guard's related maritime security directive, both announced last week. We will continue to support the Coast Guard and other DHS operational components as they amplify and execute on these new provisions.

Since our launch, the DHS Supply Chain Resilience Center has connected and collaborated across DHS components with the U.S. interagency and with private-sector partners from the transportation and trade communities. We have engaged to share our concerns with industry and seek their feedback on potential risks posed by port cranes and other port equipment and systems manufactured by the People's Republic of China. We supported the development of cybersecurity practices and conducted internal tabletop exercises to assess how the Department would respond to a disruption from these types of potential threats.

We are also engaging with international partners to learn more about their perceptions of the risk and to share our insights on practical mitigations to further U.S. supply chain resilience.

Looking ahead, we'll focus on issue areas where we can bring the full weight of DHS authorities and expertise to bear to counter PRC threats, not only today, but into the future. We are committed to effectively employing all appropriate tools to secure these vital supply chains and facilitate the trade that keeps our economy functioning.

We will work very closely within the new Cabinet-level council on supply chain resilience and with our interagency partners, including the Departments of Commerce, Transportation, and Defense, to bring a whole-of-Government approach to this vital mission.

In addition to the Supply Chain Resilience Center's work, my office is also responsible for representing the Department of Homeland Security in interagency processes to screen foreign direct investment for national security risks, namely the Committee on Foreign Investment in the United States, or CFIUS. We play a leading role in reviewing cases that implicate U.S. critical infrastructure, including our ports, in the broader trade and logistics sectors of which they are apart.

Our National security and economic prosperity are inextricably linked to a safe and efficient maritime security system, which, of course, includes our seaports. Each day, DHS plays a critical role in facilitating the safe and secure flow of millions of tons of cargo shipments into the U.S. market. We know that a port disruption can snarl supply chain and impact the delivery of goods.

That's why the Department is committed across our operational components and through the new Supply Chain Resilience Center to exercise the full range of our authorities, partnerships, and expertise to ensure Americans get the goods and materials they need.

Thank you again for the opportunity to testify, and I look forward to answering your questions.

[The prepared statement of Ms. Brzozowski follows:]

PREPARED STATEMENT OF CHRISTA BRZOZOWSKI

FEBRUARY 29, 2024

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 cybersecurity, 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 on-going 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, in-

sider 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 on-shore 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.

Chairman GIMENEZ. Thank you, Ms. Brzozowski. Members will be recognized by order of seniority for their 5 minutes of questioning. I recognize myself for 5 minutes of questioning.

During my conversations with the firm ABB, we found out that while they supply many of the motors, drives, et cetera, software for a crane, the crane built in China is the steel structure, and then the things that operate it and move and all are sometimes manufactured in China. All right. Wholly manufactured in China. Sometimes they are manufactured by other companies, some of which are Western companies, ABB being one of them. One of the things that I found most disturbing about that testimony or our conversation was that they relay to us that ABB actually ships their motors, software, hardware to the PRC, and that by contract, the CPMC makes them, gives to them, CPMC engineers will be installing that hardware, software, et cetera, that makes the cranes go.

Rear Admiral Vann, is it possible that during that process, the CPMC could be installing malware, ransomware, or Trojan horses in the software that's actually provided by, and the hardware actually provided by Western companies?

Admiral VANN. Thank you for the question, Mr. Chairman. What we have found in our activities, our operations aboard ZPMC cranes and the networks on the cranes that connect to the cranes and shore side that communicate with the cranes are either, by design, vulnerabilities of open connections. Again, I say by design, because oftentimes the monitoring of the cranes and the maintenance of the systems on board the cranes is done from a hub outside the port or in the port land side infrastructure, and then communicated to the crane through a connection. So, we have found, I would say, openings, vulnerabilities that are there by design.

What we have not found is instances, as you put it, of malware or Trojan horse type software. Our concern is with the vulnerabilities and the operators that operate these cranes, being aware those vulnerabilities exist, and then considering the report-

ing that we have heard about PRC, attempting to get onto critical infrastructure. These are obviously important nodes in our marine transportation system, sir. So, haven't found that yet. But those vulnerabilities exist to be able to access what's on the crane.

Chairman GIMENEZ. That's interesting, because the ABB folks told me that the crane system is actually like a closed system. It doesn't communicate with the outside world. I found that a little bit strange. Now you are telling me that, no, it has to communicate with the outside world, because I would figure there'd be software updates, right? Then also the crane itself communicating somewhere and saying, hey, this is bad over here, you have to replace it. So, are these cranes fully enclosed and enclosed and protected from the outside world, or do they actually communicate with the outside world?

Admiral VANN. Sir, what we have found is the cranes are designed to be able to communicate with the outside world. They can be operated disconnected from the outside world. But as you mentioned, sir, oftentimes for maintenance reasons or monitoring, some of our operators will make a connection just for that activity. Others will leave the crane disconnected and have a technician come onsite to access that data, and others will operate with the crane connected all of the time.

Chairman GIMENEZ. Very good. We also found that there were some modems installed in some cranes, and we were advised then, no, it is still a closed system. But then why would you need a modem if it is a closed system? It came with modems. So, I will leave that for another day. We can discuss that another day.

Another concern that I have is, in the United States, 80 percent of the cranes that we operate in our port system are built by communist China. If the communist Chinese decide to embargo spare parts, what would happen to our port infrastructure? What would happen to our trade if, in fact, that happened? How long will it take for, if there is an effect, for that to take hold?

Admiral VANN. Mr. Chairman, you are referring to spare parts for the cranes?

Chairman GIMENEZ. Yes. So maybe Rear Admiral Trinque, you can answer that question or somebody else who may. This is not just about cybersecurity, this is actual spare parts for the cranes.

Admiral TRINQUE. Mr. Chairman, I'm sorry. I would have to defer to someone else on how long it would take to get replacements for those cranes.

Ms. BRZOZOWSKI. Yes, I'm happy to jump in. I don't think I have a specific time frame for that particular component. But I think the larger issue here that we absolutely agree with is that we do see an over-reliance on these PRC-manufactured cranes. This is not an anomaly. We see this as a concerted effort where the PRC has proven and stated its intent to be the leading manufacturer in not only cranes like this, but other types of maritime equipment. That does introduce vulnerabilities like you are talking about, not only the cyber, but the ability to have access to the materials that are going to be necessary to maintain the smooth functioning of that equipment in our ports.

Chairman GIMENEZ. Thank you. My time is up. I now yield to the Ranking Member from Michigan, Mr. Thanedar.

Mr. THANEDAR. Thank you, Chairman Gimenez. Madam Assistant Secretary, thank you for your testimony. I appreciate the concerns that have been raised about foreign-made cranes. However, U.S. critical infrastructure and supply chains face a wide range of threats beyond cranes. How does DHS identify vulnerabilities to critical infrastructure and supply chains, and how does DHS take action based on relative risks?

Ms. BRZOZOWSKI. Absolutely. I think you have made a good point in that not only the role of seaports are indispensable to national security, but broader supply chain security, resiliency, and efforts are indispensable. DHS has a wide mission, as I mentioned in my opening statement. Trade facilitation and enforcement, protecting our cyber spaces, critical infrastructure, security and emergency preparedness and response. We have to execute on all of those missions across the totality of critical infrastructures. So not only seaports, transportation systems, but all the 16 sectors of critical infrastructure nodes.

Mr. THANEDAR. Thank you. Madam Secretary, I represent the city of Detroit. The port of Detroit is not among the largest U.S. ports and does not have any container cranes. But it is still vital to the local economy and must be protected against cyber attacks. However, small and medium-sized ports do not always have the same resources available to large ports, as they seek to invest in cybersecurity measures. What is DHS doing to ensure small and medium-sized ports are not left behind as we look to enhance cybersecurity?

Ms. BRZOZOWSKI. Thank you so much for the question. As we had said in our earlier statements as well, national security is very much inextricably linked to the smooth functioning of ports. That means not only the large ports, but many of the smaller ones that constitute our maritime transportation system. On a typical day, we see CBP processing, as I said, billions of tons of goods—I'm sorry, millions of tons of goods, and processing up to $9.2 billion of imported products. So, the value as well as the volume is quite significant.

From a DHS perspective, we are committed to across all sizes of businesses and critical infrastructure organizations, providing a whole host of free, cost-free, services that enable those organizations to take cyber hygiene, training, guidance, other types of services. We also are leveraging hundreds of advisors and subject-matter experts drawn from all sectors and all types of businesses to make sure that they are at the table in helping inform and develop those guidelines. Then finally, DHS also provides funds to State and local and private sector, not only in the maritime critical infrastructure sectors, but across those sectors, to aid in cyber preparedness, but also in prevention and testing and exercise against the whole range of hazards.

Mr. THANEDAR. Thank you so much. Arguin, I'm glad to see the administration taking board actions to enhance cybersecurity. However, some of these actions will take quite a while to show results, such as domestic manufacturing of cranes and the publication and implementation of regulations. What is the Coast Guard doing to address cybersecurity threats in the near term?

Admiral ARGUIN. Ranking Member, you are correct. The notice of parole's rulemaking that is out there. We are going to get a lot of feedback on that so that we get that right as we move forward, which will raise the bar across the entirety of the MTS. I would say that there are existing requirements to do vulnerability assessments across the MTS and assess those threats and hazards, working across the interagency to ensure that when those vulnerabilities are identified, we reach back into the facility security officers to ensure that those vulnerabilities can be closed. I think it is important to note that the Executive Order that was issued, explicitly gives us the authority to control access vessel movements, access to facilities when an identified vulnerability exists. So, I think we can take immediate action today, but I think raising the bar across the board for the rulemaking process will get a more level playing field across the MTS.

Mr. THANEDAR. Thank you, Chairman Gimenez. I yield back.

Chairman GIMENEZ. Thank you to the Ranking Member. The Chair now recognizes gentleman from Louisiana, Mr. Higgens.

Mr. HIGGINS. Thank you, Mr. Chairman. Mr. Chairman, Congress has a responsibility to observe carefully and evaluate the actions of our Executive branch and to condemn Executive actions that we believe weaken national security or injure our country. We have an equal responsibility to observe and carefully evaluate the actions of our Executive branch and to commend the actions of our White House and our Executive authorities when we believe they have done something right that's in support of national security and furthers the best interests of our Nation.

There's a rare moment when I'm going to commend the Biden administration. On February 21 this year, President Biden issued an Executive Order to bolster the security of our Nation's ports, alongside a series of additional actions that will strengthen maritime security, fortify our supply chains, and strengthen the United States industrial base. The Executive Order, the authority to respond to malicious cyber activity in the Nation's maritime transportation systems and will require the Coast Guard to report cyber threats and incidents involving a vessel, port, or waterfront facility. Further, the Executive Order invests $20 billion into port infrastructure over the next 5 years to bring manufacturing capacity back to the United States, with an emphasis on safe and secure cranes operating at port facilities.

In 2022, Chairman Gimenez introduced H.R. 6487, the Port Crane Security and Inspection Act of 2022, which would limit the operation of foreign cranes in U.S. ports. Specifically, foreign cranes are defined in that bill as those that are manufactured by companies that are subject to the control or influence of a country designated as a foreign adversary and using software or other technology that connects that crane to the port's cyber infrastructure. I was a co-sponsor of that legislation. Mr. Chairman, that sort-of effective response from Congress, as our Legislative branch, and from the White House, as our Executive branch, that's what's required for our Nation to respond to emerging cyber threats.

So, I will stand unwaveringly in the corner of the Coast Guard as it relates to your on-going and historically quite effective actions to protect American commerce and our maritime activities and our

maritime ports. The air and the sea and the land that's patrolled by our Coast Guard is under increasing threat. Therefore, the focus that Congress provides to the needs of the Coast Guard has evolved and are enhanced.

Admiral Arguin and Admiral Vann, let me just thank you for the work the Coast Guard does. As you know, Louisiana's third district, my district, produce around 60 percent of all the LNG exports shipped across the world. A 2022 Government Accountability Office report found that the Coast Guard has a shortage of approximately 400 marine inspectors. This impacts the ability to properly and effectively inspect gas-carrying vessels.

Admiral Arguin, can you speak to how military recruiting challenges are affecting Coast Guard readiness and on how the Coast Guard plans to fill those billets, including the 400 marine inspectors needed to conduct gas carrier exams?

Admiral ARGUIN. Congressman, we are actively investing in our recruiting efforts to bring in not only marine inspectors, but the entirety of the shortfall that we see, roughly 3,000 billets that are impacting our ability to deliver the effects that Congress and the American public expect.

Mr. HIGGINS. Yes, sir. So, Admiral, clearly the Coast Guard squared away. You are doing your best to fill these slots, but can you, as we have a shortage of inspectors, address your statement? What are your thoughts on using risk-based approach to conduct inspections of LNG vessels, which is highly recommended by some of us?

Admiral ARGUIN. Congressman, the Commandant's been very clear. We need to think differently about how we do our business, whether that's a resource issue or just thinking about the ability to get after ensuring compliance with existing standards or evaluating the safety of a particular vessel. A risk-based approach is something that we are certainly interested in applying based on not only resource shortfalls, but just the risk associated with those types of platforms. It gives us a different way to assess compliance and safety security of vessels.

Mr. HIGGINS. We are in support of risk-based inspections. You can count on my office to be at the Coast Guard's avail, gentlemen, ma'am, as we move forward with expanding risk-based inspections to LNG vessels. Mr. Chairman, my time has expired, and I yield.

Chairman GIMENEZ. Thank you, gentlemen from Louisiana. The Chair now recognizes the gentleman from New Jersey, Mr. Payne.

Mr. PAYNE. Thank you, Mr. Chairman. Ranking Member, and I want to thank the witnesses for joining us today. Full disclosure, as a young man, teenager, I had a great deal of reverence, still do, but at one time, I wanted to be in the Coast Guard. I guess I wasn't able to cut the mustard, so I didn't make it. But I have always had an affinity for the Coast Guard as to the other branches of the service.

So, Port Newark, located in my district, is known as the birthplace of containerization. For years, goods were located bundle by bundle onto pallets, surrounded by netting, then lifted by crane out of the ships and onto the dock, and then loaded onto trucks and trains. My father, along with several other friends and family, worked at Port Newark in their younger years. In 1956, the

SSIDLX became the world's first container ship, carrying 58 rectangular containers from Port Newark to Houston. In 1962, the world's first container turnover opened at the Port of Newark.

These achievements revolutionized global maritime commerce and trade. Times have changed, and drastically at ports across the United States. With automation and new technology, our ports are shipping and receiving more goods than ever. It is critical for us to create new guidelines to fortify our ports and maritime security framework and enhance our overall resilience in the face of evolving threats.

Secretary Brzozowski, according to DHS, one of the functions of the newly-created Supply Chain Resilience Center is to evaluate the risk to ports posed by adversarial nation-states' over-reliance on untrustworthy equipment, data extraction, and unvetted access. Port Newark uses some ship-to-shore cranes manufactured by ZPMC that may potentially pose cyber threats. Are there any examples where over-reliance on ZPMC cranes has led to vulnerabilities to port security?

Ms. BRZOZOWSKI. Thank you for the question. Thank you as well for that shout-out about the history of containerization and how it is revolutionizing the shipping industry. I think we really are, and agree, at such an inflection point right now. Particular to the presence of these PRC-manufactured cranes and whether we have seen any specific vulnerabilities, not to my knowledge. But I think as we are taking a close look at this issue, it is because of the potential for such a risk and the known exploitation by the PRC of critical infrastructure, even domestic critical infrastructure sectors.

Mr. PAYNE. Yes, I believe that there are 200 cranes that they have had, and I believe the Coast Guard has made a check of 92 of them and haven't found any problems. The SCRC plans to conduct at least two tabletop exercises in 2024 to test the resiliency of the critical cross-border supply chain with other U.S. Federal agencies, foreign governments, and industry. One critical component that I believe could be addressed with exercises and engagement and coordination with local governments. Will opportunities be presented for local governments to participate or gain knowledge so that they are well-prepared in the event of an incident?

Ms. BRZOZOWSKI. Absolutely. Local, State—local officials, as well as State and local critical infrastructure organizations—are going to be a key point of any tabletop exercises and will certainly be part of the ones that we are planning under the Supply Chain Resilience Center.

Mr. PAYNE. Thank you very much, and I yield back.

Chairman GIMENEZ. Thank you, gentleman from New Jersey. The Chair now recognizes the gentlewoman from Florida, Ms. Lee.

Ms. LEE. Thank you, Mr. Chairman. Building domestic infrastructure capacity is critical to reducing our reliance on foreign-made machinery, safeguarding our seaports from debilitating cyber attacks, and maintaining functional equipment. Thoughtful consideration of modernization of procurement policies to benefit the utilization of domestically-manufactured equipment is critical to mitigating our reliance on cranes produced by foreign actors. Due to cost, regulations surrounding procurement and other limitation, nearly all cranes used in U.S. seaports are manufactured in China.

This includes 2 of the 5 cranes at Port Tampa Bay. I appreciate the thoughtful discussion and testimony we have heard already today about this issue and how we can be working together to mitigate these threats and ensure that our ports are safeguarded.

I would like to follow up, Secretary Brzozowski, with you on this question. As Members of Congress, we spoke a little bit earlier about supply chain as it relates to cranes. I'm interested in your thoughts on what we can be doing as Members of Congress to work with DHS to help build domestic infrastructure capacity for components of the supply chain as it relates to our cranes.

Ms. BRZOZOWSKI. Thank you very much for the question. Again, I think—thank you for your leadership, and I think we agree that there's very serious vulnerabilities associated with an over-reliance on any type of supply chain component that's not produced here in the United States. The Department of Homeland Security is not in the position of providing a lot of the incentives to incentivize domestic production beyond our partnerships with them to make sure that they are understanding that being part of a secure and resilient supply chain is something that's going to afford them opportunities. We know that if an adversary is exploiting some of these systems, the port can completely shut down. That's why we are working very closely with the Department of Transportation, the Department of Commerce, on some of these incentive programs. So, I think full funding of those programs, communication out to your constituencies about the availability of these programs, and an amplification of the vulnerabilities that we are seeing from a security perspective would just raise the attention and promote further production of some of these capabilities.

Ms. LEE. Thank you. Admiral Arguin, one of the other things that we have heard mentioned today is the Executive Order that the President recently signed to empower the Coast Guard to issue directives regarding cranes manufactured in the PRC. Can you touch on what actions, how crane operators have responded, and how this is affecting your operations?

Admiral ARGUIN. So, ma'am, the maritime security directive required notification of affected crane owners and operators within 48 hours. We have touched base with each one of those crane operators. They've acknowledged that the maritime security directive applies to their operations. So, we're now continuing the conversation about what needs to be done within the elements of the sensitive security information to close those vulnerabilities. If there are questions that come up about the specific details, then my colleague at the Coast Guard Cyber will be able to support, or others that have technical supporting role, we'll be able to help them close those vulnerabilities. Then there's a window that we will have confirmation that all of those vulnerabilities have been closed within those ports.

Ms. LEE. Admiral Vann, would you add to that response for us?

Admiral VANN. Yes, Congresswoman. As was alluded to, if it is determined that vulnerabilities do exist, as I mentioned earlier, open doors in the network, on the cranes or to the cranes, the services that we provide from Coast Guard Cyber Command, assess those vulnerabilities, can hunt to see whether or not there's adversarial action on the crane network and then help the operator

eradicate it. There are other sources of these types of services. Some companies have them internal to their organizations, others can hire this kind of help, but we can validate behind someone else's actions. We actually will deploy out into the port, onto the crane network, and we are doing that now. As was mentioned, we have assessed almost half of the PRC manufactured cranes in the country already.

Ms. LEE. Thank you. Mr. Chairman, I yield back.

Chairman GIMENEZ. Thank you to the gentlewoman from Florida. Now the Chair recognizes gentleman from New Jersey, Mr. Menendez.

Mr. MENENDEZ. Mr. Chairman, Mr. Ranking Member, thank you for convening today's hearing on port cybersecurity and for allowing me to waive on. To our witnesses, thank you for being here. In my time on the Subcommittee on Cybersecurity and Infrastructure Protection, I have been proud to work with our Federal partners and private-industry stakeholders to improve the security of our critical infrastructure. New Jersey's 8th Congressional district is home to the largest port on the East Coast, where hundreds of billions of dollars of goods move each year. The smooth and effective movement of cargo through the Port of New York and New Jersey is critical to our economy, both regionally and nationally. I'm glad to be able to participate in today's hearing as we discuss how we can continue to keep our ports safe from cyber threats.

Secretary Brzozowski, in your testimony, you mentioned that the Supply Chain Resilience Center within DHS has begun building partnerships with foreign governments. Our international partners are going to be facing many of the same vulnerabilities as our own ports, including those related to ZPMZ-built cranes and the full range of cyber threats. How is DHS working with our international partners on cyber threat information sharing related to our ports and their ports?

Ms. BRZOZOWSKI. Maybe I will provide a broad overview, but then would defer to my Coast Guard colleagues on the actual cyber-specific information sharing. Through the Supply Chain Resilience Center, we are working with a variety of foreign nations on looking at this particular threat, comparing notes and seeing what their perspective is, and also discussing particular mitigations. We are also working to identify other countries that have models of Supply Chain Resilience Center that could afford a good template for not only what the Department of Homeland Security is doing, but how we are working with our interagency partners in Transportation, Commerce, and the Department of Defense. Having the center be able to work with our interagency colleagues and with the private sector is very important. But also having our center be able to connect with similar centers internationally and develop early warning systems and share information about not just cyber threats, but the movement of goods, shipping trends, logistics information, and be able to not only predict and mitigate, but also practice for and exercise our capabilities in terms of enhancing the resilience against any type of threat.

Mr. MENENDEZ. Have you identified any models or any of our international partners who are sort-of perhaps ahead of where we are on identifying and addressing these challenges?

Ms. BRZOZOWSKI. We have had great conversations with a range of international partners, one with our colleagues in Finland stands out. They have maintained a Supply Chain Resilience Center that has kept domestic production and has exercised against a range of hosts, you know, throughout the Cold War, since World War II. You know, they are operating on a different scale than we are. But many of the models, the frameworks, and the ideas are ones that we are finding very valuable and informative.

Mr. MENENDEZ. Appreciate that. We have talked a lot in our Cybersecurity Subcommittee, this Congress, about how to streamline reporting requirements to make sure they are effective. The Coast Guard seems well-positioned to lead in this area because of the existence of the National Response Center, which is the single reporting point for physical security breaches at ports and has a mature process for passing that information to Federal, State, and local agencies. For any of the witnesses that would like to take this, could the Coast Guard leverage the existing National Response center to streamline cyber incident reporting?

Admiral ARGUIN. Congressman, we currently use our National Response Center as the single point for reporting information related to maritime cyber incidents. There is an on-going effort by CISA to try and harmonize that across the interagency, and we are participating in that to ensure that there's a seamless connection to two Federal entities that need to know about incident reporting or incidents that have happened within other segments.

Mr. MENENDEZ. Appreciate it. Sort-of just to follow up on that, I want to make sure that we are preparing for that information sharing to go both ways so that our ports have access to timely, actionable intelligence about cyber threats. How does the Coast Guard share reported threat information with industry participants, and how does the Coast Guard work with partners like CISA, the MTS, or ISAC to ensure effective information sharing?

Admiral VANN. Congressman, I will take a stab at that one.

Mr. MENENDEZ. Thank you.

Admiral VANN. So we absolutely do provide from Coast Guard Cyber command resources to include current information on threats that's available to operators imports. Additionally, working across the interagency with CISA and others, we will produce maritime cyber alerts as timely as possible. So, those are kind-of as-needed as threats emerge. Then, we are a member of the intelligence community, so we are working with other agencies and DoD across intel, and we have had examples of declassifying higher classification information and then making that available to port operators. Finally, you mentioned the ISAC. We absolutely cooperate, share information. They do a good job of pushing it out across all operators in the system.

Mr. MENENDEZ. Appreciate that. I yield back.

Chairman GIMENEZ. Thank you to gentlemen from New Jersey. The Chair now recognizes the gentleman from New York, Mr. D'Esposito.

Mr. D'ESPOSITO. Thank you, Mr. Chairman, Mr. Ranking Member, thank you for allowing me to waive on this morning. Thank you to the panel for being here and for your service to this country. I represent New York's fourth district, which is Nassau County on

Long Island. I know how important the Port of New York and New Jersey is to not only New York, but our region and, of course, this country as a whole. According to a report by the Port Authority of New York and New Jersey, this port is the largest container port on the East Coast, moving hundreds of billions in goods each year.

This is really an open question to any of you. In 2022, China was by far the No. 1 country of origin for goods coming into this port. Can anyone speak roughly to the size of the physical Chinese presence at both the Port of New York and New Jersey, and specifically other ports on the East Coast? Not all at once.

Ms. BRZOZOWSKI. Not specifically, no. I mean, this is very much the issue that under the new Supply Chain Resilience Center, we are taking a close look at to get an understanding of not only the dominance in port cranes, but looking across other types of port equipment and then looking across broader infrastructures.

Mr. D'ESPOSITO. OK. So, I think we would agree that there is a presence. Obviously, the goods are the presence, and they have a physical presence at the ports. So, are there any implications for our cybersecurity due to their large presence, not only physically, and the goods in the ports of New York and New Jersey and the Northeast?

Admiral VANN. Congressman, I would just say that what we experience when we operate on critical infrastructure networks, in ports, on operational technology and information technology networks, I guess I would offer, there are a number of vectors by which access can be gained. It could be physical access. It could be remotely through networking and communication lines that come in from the outside, or conceivably it could be local physical presence that then either connects through a physical connection or a Wi-Fi connection to a network. So, that doesn't directly answer your question, but certainly presence as a threat vector, if that does.

Mr. D'ESPOSITO. Right. So, I think that it is important to realize our ports. Obviously, there's so much that goes into the logistics of the ports, whether it is the physical port itself, the trucking industry, the warehousing, the cargo that's in the port. Can you just describe the implications, because I think it is sort-of hard to understand, the implications of even what a short-term halt would do to a port like the Port of New York and New Jersey.

Admiral ARGUIN. Congressman, what I would maybe try and take sort-of the view is, any disruption, cyber or otherwise, hurricane, anything that would cause a ripple in that very tightly fine-tuned system will have really diverse impacts. So, part of what each local sector commander, captain of the port, is focused on each and every day with their teams is to ensure that are we looking at the right things to determine whether or not those disruptions are predictable? If they are, what can we do to minimize that disruption downstream? You know, it's one aspect of the marine transportation system is to get the cargo to the port. There's an entire rest of that conversation that will be impacted downstream. So, we are hyper-focused on that. I know that the Supply Chain Resiliency Center is also looking at that to ensure that that disruption is minimized to the extent possible.

Mr. D'ESPOSITO. Right. So specific to, again, talking about responses and shutdowns at ports. Obviously, to your point, there's so much that goes into preparing and mitigating, and we always want to ask ourselves, are we better off today than we were yesterday in preparation for whatever the inevitable is? So how fast would the Coast Guard be able to respond to an incident at the port? Specific to New York and New Jersey, is it almost instant?

Admiral ARGUIN. So we maintain a 24/7 presence in all ports. So as soon as we are aware of the challenge, we'll decide which teams need to be involved at understanding the impact of that, and then what we need to do to minimize that disruption.

Mr. D'ESPOSITO. Mr. Chairman, my time has expired. I yield back.

Chairman GIMENEZ. Thank you to the gentleman from New York. Now the Chair recognizes gentleman from Texas, Mr. Pfluger.

Mr. PFLUGER. Thank you, Mr. Chairman, and thanks for allowing me to waive on. I appreciate the witnesses for your service. Also, during this time, through our own investigation here on Capitol Hill and through your efforts, I think every American should be concerned about even the possibility of the vulnerability that we see in our ports, with regards to the Chinese Communist Party and their use of trade to facilitate many different nefarious actions.

So, I will start with Admiral Trinque. To the extent that you can, can you share what policies or plans that TRANSCOM has taken under the National Port Readiness Network that use Chinese manufactured port equipment and technology to make sure that we are secure and what those vulnerabilities are?

Admiral TRINQUE. Congressman, thank you very much for the question. Our strategic seaports are critical to our ability to project and sustain the joint force. So, the National Port Readiness Network allows us, at an interagency level, to assess and remediate risks in those ports. Specific to the technology to which you refer, in our strategic seaports, when we deploy out of an Army unit, for instance, out of our strategic seaports is generally not using those cranes. It is generally using other types of vessels, other modes of transport. Additionally, in our strategic seaports that do have those cranes, there are other cranes that could be used. So, our current assessment is none of our strategic seaports right now are wholly dependent on those cranes.

Mr. PFLUGER. OK, I will go to Admiral Vann. During our investigation, we learned that ZPMC manufactures many of its ship-to-shore cranes at Shenzhen base, which is also very close to the Shenzhen Island, which is close to where the PLAN produces a lot of its warships. Obviously, there's the proximity, and just knowing how many of these companies operate inside China is concerning. So, No. 1, are you aware that the ZPMC ship-to-shore cranes used by U.S. ports are manufactured near the PLAN ship-building site?

Admiral VANN. No, Congressman, I was not aware that the construction of the cranes occurs at a location close to a PLA Navy site.

Mr. PFLUGER. Does anybody on the panel want to take a stab at this or is this something that y'all are aware of?

Admiral TRINQUE. Congressman, I was not aware of that. I don't know that that increases the level of risk, because I think we view the proliferation of Chinese technology in our seaports as a potential strategic risk regardless of where in the PRC they are constructed.

Mr. PFLUGER. Yes, I mean, it is hard not to think that it wouldn't increase the risk if their proximity was either co-located or on the same island, or that they share either some sort of trade secrets or intellectual property. There are some of these things that we don't know, so I maybe disagree with you slightly that that wouldn't increase the risk. But I guess the question here is, what are we doing about those types of things, whether geographically co-located or there's a network of leadership that is tied together? What are we doing as a U.S. Government to either prevent that or stop those normal bills? It looks like you want to answer?

Admiral ARGUIN. So, I won't really dive into stop the manufacturer piece. That's really outside of my lane. What I would say is the Executive Order, specifically with respect to Chinese manufacturer cranes, required certain things to be done to close known vulnerabilities and assess those vulnerabilities to ensure that they cannot be exploited. Then our proposed rulemaking would require a vulnerability assessment across all modes, regardless of where something had been manufactured, to understand where there may be exploitable connectivity, and then requirements that would close those down.

So, to some extent, regardless of where you manufacture something, we would understand where there were potentially doors were open and so that we could close those doors to prevent some sort of nefarious activity.

Mr. PFLUGER. OK, talking about the Executive Order, and I will go to Ms. Brzozowski. Was this Executive Order in any way linked to Volt Typhoon and the malicious activity that Microsoft, I guess, first allegedly reported on?

Ms. BRZOZOWSKI. I actually defer to my Coast Guard colleagues on that who are aware of all the details.

Admiral VANN. Congressman, I'm just happy to talk a little bit about that particular threat. That actor is a threat that uses a technique called living off the land. These are activities on a network that are not easily recognizable because they get on a network and then use standard activities that occur in network traffic all of the time. So, what it requires us to do, as we look for adversaries, is to look for behavioral patterns. So, a significant amount of analysis after we look at a network.

Back to the question of the EO. What the EO really does, again, is allow a captain of the port, if it is determined that there is a threat or there's been some disruption because of a cyber intrusion, to take action to, maybe in this case, in your example, to secure a crane or secure a terminal until such time that the operator, maybe with our assistance, at least with our validation, takes action to secure that particular node of the system.

Mr. PFLUGER. Thank you. Mr. Chairman, my time has expired, but I commend you for this hearing. Obviously, 5 minutes is not enough to dig into all the issues. But thank you for allowing me to waive on.

Chairman GIMENEZ. Thank you, gentlemen from Texas. The Chair now recognizes the gentleman from California, Mr. Garcia.

Mr. GARCIA. Thank you, Mr. Chairman. I'm proud to represent a district that includes the Port of Long Beach. It is one of the largest ports in the United States and the second-largest container seaport. The Port of Long Beach is a city department in Long Beach, and when I was mayor, for the last 8 years, the harbor department was a huge part of the work that we do in the city and, of course, across California and the West Coast. I'm also proud to co-chair the Congressional Ports Caucus, and security of our ports is incredibly important and a top priority for us and the work that we do. We know that the port's impact on the economy is critical. Of course, we saw its impact when we had the supply chain crisis just not long ago. My port alone handles trade valued over $200 billion every year, and we support 2.6 million jobs throughout the supply chain and throughout different types of trade and transportation jobs across the country.

It is great to see bipartisanship today on this issue. I will love to add that I think President Biden has been a great leader on issues around ports and security. I think the investments being made in the infrastructure bill are significant, and he's also taken reasonable and common-sense steps to improve maritime security. Last week, of course, he had his Executive Order, which got support from both sides of the aisle as well. Chairman Gimenez and I also work together as former mayors as co-chairs of the Peru Caucus, which is nice to say, also to have bipartisan support there as well.

Now, under the Executive Order, the U.S. Coast Guard will have the authority to respond to cyber attacks or espionage in the supply chain with new standards. We will also require reporting of cyber incidents or active cyber threats, endangering vessels, harborous ports, or other waterfront facilities. We know this is critical because we know that the maritime supply chain include many overlapping companies and actors as well. Now, our hearing today, I know, is focused on cranes, which is critical and surely has to be discussed and investigated. But we know that cyber attacks can hit anywhere in the supply chain, including at port terminals or vessel communications.

Rear Admiral Vann, I'm sure you are familiar with the history of ransomware attacks which have impacted port operations, including back home in California and around the world. Can you speak more about how President Biden's Executive Order will increase security at other parts of the supply chain, from terminal operators to other important communications networks?

Admiral VANN. Yes, Congressman. Again, what the Executive Order does is give that local captain of the port the ability to either react to a known threat or respond to an actual attack. Not just to cranes, but to all of the operational technology in the marine transportation system, and business systems as they apply to impacting the operations of ports. So, in our work in the Coast Guard Cyber Command, we go about the business of assessing the vulnerabilities that exist, about notifying partners, that we talked about, with threat information and then about locating malicious activity and helping port partners eradicate it. Again, the Execu-

tive Order gives that local captain of the port the opportunity, the ability to keep the port safe and secure while a cyber threat is addressed.

Mr. GARCIA. Thank you. I want to also, just to add on that rear admiral, the issue of the way automation is also changing our needs around being cyber secure. Certainly, it is impacting not just cranes but other types of vehicles and equipment at our ports and harbors. Do you see that the increase in automation, which there is some concern about and certainly from the IW dock workers and others, does that actually increase our kind-of vulnerability to attacks and to some of these concerns being shared today?

Admiral VANN. Thank you, Congressman. I have kind-of been waiting for this question. Absolutely. As we increase automation, while it brings efficiencies, it increases the terrain, the cyber terrain that we must protect. The point I really want to make here is that all of us, whether it is government, private companies that are operating in the ports, all need to take the vulnerabilities that are created by this increased surface, this threat surface, that's now there with increased automation, need to take that very seriously, make it part of their calculus in securing the system.

Mr. GARCIA. I think that's absolutely right. That's one of the concerns that I share also with kind-of automation that's not really gone through a real process with the workers in the community and cyber experts and what we are seeing. Just last, just more of a comment than anything else. So, I have been to China a few times as mayor of Long Beach and met with port operators and companies there. It is important to remember that China is absolutely competitive with the United States. They are in it to beat us in every single way. We want to make sure that we are always ahead. It is also critical to note that China is our single largest trading partner in the United States, on the West Coast especially. Our ports, all on the West Coast, depend on Chinese trade, and so, we must look at China both as a competitor but also a strategic partner when it comes to commerce. West Coast ports would collapse without Chinese trade, and millions of jobs would be lost, certainly in districts like mine and others along the West Coast as well. So, we have to, I think, both balance those while continuing to push and understand the real threats that China poses to our economy and certainly to cybersecurity.

With that, I yield back.

Chairman GIMENEZ. Thank you from gentlemen from California. I will be open to a second round for those who want to stick around. So, there are some other questions that I want to ask. I know you were expecting it, but here we go. All right.

As the testimony is, you know, as I'm listening to the testimony my mind goes somewhere else. I know about cybersecurity, but my mind goes to actual physical impediments. So, none of you, I don't believe, have the answer to my question. What would happen if China somehow embargoed spare parts, maintenance, et cetera, of cranes? What would happen to our ability to move our commerce? Because 80 percent of the commerce that comes in the United States through the seas, actually, somehow a Chinese crane touches it, because we have 80 percent of the cranes in this country are Chinese-manufactured.

Another question that I have is, how do they get there? How were they able to achieve such dominance, and are they increasing their dominance around the world, and how can we combat that? Not sure, again, that any of you have the answer to that question. But maybe you have the answer to this question. I have recently came back from Peru, and a CODEL down to South America, Panama. Interesting that the canal that we built has Chinese control port on the Pacific side and on the Atlantic side. They are building a new port down in Peru for the Peruvians. The Peruvians are going to ask for another port down in south Peru, and hopefully we can bid on it. But something tells me somehow that the Chinese, the CCP, are going to underbid the United States. Is it possible, as a possibility—and they are building airports and seaports around the world. Is it possible that without safeguards, that our trade can actually be disrupted across the world with the dominance of the crane, not only the cranes, but also the ports in a nefarious fashion, so that Chinese manufactured goods, et cetera, flow very smoothly, but somehow American manufactured goods and trade don't flow quite as smoothly? Is that a possibility?

Ms. BRZOZOWSKI. I'll take that and say, yes. I think it's not only a possibility, but something that we're seeing play out around the world. It's no secret that China has both the capability and the intent to challenge the rules-based trade system, and they are leveraging all instruments of their national power to do so. They're looking to gain access not only to technology and data, and in particular the vulnerabilities that we're talking about around the cranes today, but engaging in a number of other practices to undercut American workers and businesses. We're seeing an influx of production of fentanyl through American ports, if you're talking about physical ports, we're seeing a use of vile practices associated with forced labor to undercut the competitiveness of United States and other global companies and bringing goods to market. That are not only made in a means that are very contrary to U.S. values, but undercut, as I said, legitimate businesses that can't compete in that type of situation. We're also seeing that we're blind to economic influences coming in through investments. I spoke that DHS is part of the CFIUS committee, the Committee on Foreign Investment in the United States, and we're taking a very, very close look at investments, particularly in our critical infrastructure sectors.

Chairman GIMENEZ. I take concern with their zeal in creating and investing and actually manufacturing, creating the infrastructure that they need in order to create ports, airports, et cetera, that will dominate trade around the globe. They do this, it is really not a great value for those countries. It is a cheap price, but not a great value, and I will explain why. They will give a cheaper price, but then they'll bring the labor from China to do the work, which in essence, means that that country's capital is actually leaving, going to China versus what we do. Usually we bring our expertise, but the actual work force for that infrastructure is actually from the country, which means more of that money is actually invested in the country. So, this Belt and Roads Initiative caused me great concern. It is not just about the cranes, it is about the entire—and they do it in a very holistic fashion, and they are very committed

to that. So, I share great concerns about that. So, I will yield now to the Ranking Member from Michigan, Mr. Thanedar.

Mr. THANEDAR. Thank you, Mr. Chairman. Yesterday, Congressional leaders announced a plan to address Government funding for the remainder of the fiscal year. I'm hopeful that we can avoid a costly and unnecessary Government shutdown. But given how elusive a funding agreement has been, I am not making any assumptions until a bill is passed and signed by the President. The last Government shutdown in 2019 had a dramatic and lasting impact on the Coast Guard, among other agencies, and a shutdown now would have a similar effect. I want to ask each one of you, any one of you, how would a Government shutdown affect your agency's work force and mission, in general, and port security in particular?

Admiral ARGUIN. Ranking Member, the uncertainty associated with a Government shut-down or continuing resolutions certainly has an impact on our ability to continue to purchase and bring to bear new technologies that are going to be important in protecting the Nation's ports. It also has a negative impact on our ability to recruit and retain. We talked earlier about the challenges that we are currently having to bring in new talent, the talent that's necessary to deliver on the services that you and the American public expect. You mentioned 2019, 35-day shutdown where the Coast Guard was not getting paid, that is still having reverberating effects on our existing work force, on our ability to retain individuals. So, that will not help us bring in that talent that we need.

Mr. THANEDAR. Thank you. Anybody else?

Ms. BRZOZOWSKI. Yes, thank you for the question. I will say without equivocation that any lapse in Federal funding disrupts the vital work of the department and will leave Americans less safe as a result. Three out of 4 DHS employees would be required to work without pay should there be a shutdown. This includes enforcement officers at the borders, analysts, investigators, and, of course, the men and women of the U.S. Coast Guard.

Mr. THANEDAR. Thank you, Madam Secretary. Admiral Arguin, last week, the Coast Guard issued a notice of proposed rulemaking to enhance cybersecurity by requiring port owners and operators to implement a wide range of measures. This proposal builds upon a series of security directives TSA has issued for various modes of transportation over the past few years, and it represents a change from the voluntary approach the Coast Guard has previously taken in issuing cybersecurity guidelines. Why did the Coast Guard decide to initiate the rulemaking process rather than continuing to rely on voluntary standards?

Admiral ARGUIN. Ranking Member, I think the entirety of this hearing has kind-of highlighted the increasing vulnerabilities, the increasing connectedness of systems within the marine transportation system and those vulnerabilities and its long-term consequences of not doing something requiring vessels and facilities that operate in that system to have an elevated standard. We are very much interested in getting feedback on whether or not that standard is going to be effective, but we also recognize that whatever standard gets put in place is going to have to regularly evolve, given the emerging threats.

Mr. THANEDAR. Thank you. How did the Coast Guard coordinate with TSA in developing the proposed rulemaking? How do the Coast Guard's requirements mirror those issued by TSA and how do they differ?

Admiral ARGUIN. Ranking Member, so every 2 weeks we have a cybersecurity interdepartmental conversation about where each of the interagency rulemakings are in the process. So, we were looking to harmonize that just within the Department. Then we also participate with CISA's Cyber Incident Reporting Council to ensure that we have got harmonization within the Department. But there have been regular conversations about where certain things are required. I mean, in fairness, cybersecurity is not inherently special to the maritime. Those same systems and vulnerabilities exist across all modes, all sectors. So, we want to make sure that those same vulnerabilities are being closed across each of those so that work will continue.

Mr. THANEDAR. Thank you. Chair, I yield it back.

Chairman GIMENEZ. Thank you to the Ranking Member. Mr. Payne, you are recognized.

Mr. PAYNE. Thank you, Mr. Chairman, Ranking Member. Last week, the Biden administration announced billions in funding to support domestic crane manufacturing to strengthen our critical infrastructure resilience at ports across the country. I am very happy to see the President's effort in bringing a lot of this manufacturing back home. We passed the CHIPS Act to make sure that we have the chips that we need and don't have to rely on foreign adversaries. Also, it is good to see that they are bringing back the crane composition. We need to manufacture here at home. The Biden administration has taken many steps in order to secure the equipment that we need at home and not rely on foreign actors.

So, Assistant Brzozowski, as the administration makes these needed investments, how will the SCRC ensure opportunities are made available to local business, particularly minority-owned-operated businesses, to serve as contractors or subcontractors?

Ms. BRZOZOWSKI. Thank you very much for the question. The Supply Chain Resilience Center is working across the interagency to identify the areas where, from a security perspective and a resilience perspective, we would like to see domestic production increase. We work very closely with the other agencies that are going to be responsible for administering those funds that go out to incentivize some of that return of production, that includes the departments of Transportation and Commerce. Of course, we would love to see and very much believe that local businesses, local critical infrastructure operators, will be a key part of bringing some of those production capabilities back under some of these incentive programs.

Mr. PAYNE. Thank you. Rear Admiral Arguin, considering that the Port of Newark is a crucial hub that drives economic activity both locally and nationally, and I ensure it remains that way, how will the Coast Guard work with ports to ensure that they have full understanding of the required cybersecurity measures and to check for compliance?

Admiral ARGUIN. Congressman, so Captain Zeita Merchant, who's the current sector commander of captain of the port, regu-

larly engages with industry stakeholders within her operational area. Her staff have been engaging with, not only the facilities that have cranes that could be considered underneath this Executive Order, but across the board, any one of those facilities that has a potential vulnerability that could disrupt the flow of commerce within the Port of New York, New Jersey, she is hyper-focused on.

Mr. PAYNE. Excellent. Are there grant funding that's available for ports as they work to enhance cybersecurity?

Admiral ARGUIN. Yes, sir. Each year, FEMA puts on port security grant programs. The local sectors, captains of the port, support bringing in industry stakeholders, evaluating those proposals against potential buy downs of risk, and then we provide those recommendations to FEMA for a decision on whether or not those particular grants would be supported.

Mr. PAYNE. Well, thank you for that. I thank you for your answers from all the panel. Thank you for your service to this country. With that, I will yield back.

Chairman GIMENEZ. Thank you, gentlemen from New Jersey. The Chair now recognizes gentleman from California, Mr. Garcia.

Mr. GARCIA. Thank you. Just to circle back, I'm trying to remember if someone knows the company that actually produces most of the Chinese cranes is ZPMC, I believe, if that's correct, and maybe this was discussed earlier. So interestingly enough, I have been to the ZPMC factory in China, when I was mayor, and especially because so much of our economy was port-related and working. They obviously have a huge American presence as well and are very present in the Long Beach-Los Angeles area. Of course, their operations are immense and incredibly impressive.

So, I just want to add to what my colleague was saying is the one thing that I took away from that experience was how lacking our ability to produce this level of infrastructure is in the United States. We have nothing near ZPMC's kind of output because they are producing globally. My concern would also be, is that this is not only a national security issue for the United States, where we import numerous ZPMC cranes, but it is a national security issue across the world, where every port that they are building or every crane that's going to another port, the Chinese do have influence or the ability to possibly have disruptions there.

So I just want to add that anything that we can do as a committee or as Members to assist in encouraging the production of cranes and port manufacturing here in the United States is something that we must do. I'm not sure if there's a comment on that from anyone.

Ms. BRZOZOWSKI. I'm going to jump on that, because I would love a second bite at the apple of a prior question about what Congress can do. Of course, as we stand up the Supply Chain Resilience Center, we are pulling from existing resources within the Department. We would love to work with Congress to fully fund that effort and ensure that we have got the capabilities, as do our other departments, that we'll be coordinating with to deep dive, have that analytical visibility, the research capabilities, and to be able to really create an agile and responsive capability in service of ensuring supply chain resilience.

Mr. GARCIA. Thank you. Then I have one question that's unrelated, it is about the *Conception* fire, and I want to touch on this topic. In Southern California, the *Conception* fire, obviously, for those that don't know, was a dive boat that caught fire and sank off the Santa Cruz Island, off the coast. Thirty-three passengers and 1 crew member were killed when a fire broke out below decks. Worst maritime disaster in California in over 150 years. We obviously want to make sure that this doesn't happen again. The NTSB's report on the accident concluded they had a safety management system—I'm sorry, they concluded that had a safety management system been in place, the owner operator of *Conception* could have identified unsafe practices and fire risks on the boat and taken corrective action before the catastrophe and loss of life occurred.

We know that the Coast Guard obviously is involved in looking at this. The Coast Guard since 2021, we believe, has not really been producing as quickly as we would like to see the information. This was 3 years ago. Last year, I asked about making progress on the rulemaking and was told, "The Coast Guard is actively working on the notice of proposed rulemaking for the safety management systems on passenger vessel rulemaking."

Admiral Arguin, it is almost been a year since then. I can best tell there's been no real progress made, but maybe there has been. I know this falls under your Command for Prevention Policy, so I'm just wondering when the Coast Guard will issue a proposed rule for safety management systems for passenger and small passenger vessels?

Admiral ARGUIN. Congressman, so the process to evaluate comments and to generate a rule is complex and can take a while. Especially when you get a number of comments that you need to adjudicate. We are continuing to work through those. But I would say that we have implemented a number of other measures since the *Conception* fire that have reduced risk for those particular types of platforms. So, we're actively working to get that safety management system rulemaking finalized. But I think large across the board, the small passenger fleet is a safer fleet today.

Mr. GARCIA. I know that we hear the *Conception* families. Of course, there's just a lot of hurt and interest in getting that resolved. The NPRM says possibly later this year we'll get some type of report or additional implementation, do you think that date is going to stick, Admiral?

Admiral ARGUIN. Sir, I'm not a betting man. I would say that the challenges of getting a rulemaking are not something that we are slowed down by, but we're continuing to press forward to try and get a rulemaking on the street as soon as possible.

Mr. GARCIA. Thank you very much, sir. Appreciate that.

Chairman GIMENEZ. Thank you, gentlemen, from California. Mr. Garcia, let me say that the importance to restore heavy manufacturing back to the United States that's critical to our National security, is something that both sides fully are in agreement with. We don't agree on too many things, but on that we do.

So, again, I want to thank the witnesses for their valuable testimony and the Members for their questions. The Members of the subcommittee may have some additional questions for the wit-

nesses, and we would ask the witnesses to respond to these in writing. Pursuant to Committee Rule VII(D), the hearing record will be held open for 10 days. Without objection, this subcommittee stands adjourned.

[Whereupon, at 11:50 a.m., the subcommittee was adjourned.]