EVALUATING HIGH-RISK SECURITY VULNERABILITIES AT OUR NATION’S PORTS

HEARING
BEFORE THE
SUBCOMMITTEE ON TRANSPORTATION AND MARITIME SECURITY
OF THE COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES
ONE HUNDRED EIGHTEENTH CONGRESS
FIRST SESSION
MAY 10, 2023
Serial No. 118–10
Printed for the use of the Committee on Homeland Security


U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2023
## CONTENTS

### STATEMENTS

<table>
<thead>
<tr>
<th>Speaker</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Honorable Carlos A. Gimenez, a Representative in Congress From the State of Florida, and Chairman, Subcommittee on Transportation and Maritime Security:</td>
<td>Oral Statement</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Prepared Statement</td>
<td>2</td>
</tr>
<tr>
<td>The Honorable Shri Thanedar, a Representative in Congress From the State of Michigan, and Ranking Member, Subcommittee on Transportation and Maritime Security:</td>
<td>Oral Statement</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Prepared Statement</td>
<td>4</td>
</tr>
<tr>
<td>The Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:</td>
<td>Prepared Statement</td>
<td>4</td>
</tr>
</tbody>
</table>

### WITNESSES

<table>
<thead>
<tr>
<th>Witness</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Prepared Statement</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Prepared Statement</td>
<td>12</td>
</tr>
<tr>
<td>Mr. John “Neal” Latta, Assistant Administrator, Enrollment Services and Vetting Programs, Transportation Security Administration, U.S. Department of Homeland Security:</td>
<td>Oral Statement</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Prepared Statement</td>
<td>16</td>
</tr>
</tbody>
</table>

### APPENDIX

<table>
<thead>
<tr>
<th>Question From Speaker</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questions From Honorable Robert Garcia for Wayne R. Arguin, Jr.</td>
<td>33</td>
</tr>
<tr>
<td>Questions From Chairman Carlos Gimenez for Eric Goldstein</td>
<td>33</td>
</tr>
</tbody>
</table>
EVALUATING HIGH-RISK SECURITY VULNERABILITIES AT OUR NATION’S PORTS

Wednesday, May 10, 2023

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

The subcommittee met, pursuant to notice, at 2:02 p.m., in room 310, Cannon House Office Building, Hon. Carlos A. Gimenez (Chairman of the subcommittee) presiding.


Mr. GIMENEZ. The Committee on Homeland Security, Subcommittee on Transportation and Maritime Security will come to order.

The purpose of this hearing is to receive testimony from the distinguished panel of witnesses who will speak to high-risk security vulnerabilities at our Nation’s ports and actions Congress can take to improve port security and ensure public safety.

I now recognize myself for an opening statement.

This subcommittee’s hearing today will discuss security vulnerabilities at our Nation’s maritime ports. Ports are essential to our way of life in the United States. The United States is a maritime nation with 361 commercial ports, 25,000 miles of navigable channels, and 95,000 miles of shoreline.

Maritime shipping is a critical component to our Nation’s economy. Approximately 90 percent of imports and exports enter and exit the United States by ship, generating over $4 trillion of economic activity every year.

Maritime ports are also essential to our military’s ability to respond to threats and project power overseas. During Operations Desert Shield and Desert Storm, the Navy’s Military Sealift Command delivered more than 12 million tons of equipment, vehicles, and material facilitating a massive coalition force that ejected Saddam Hussein’s forces from Kuwait. Our military cannot operate for sustained periods of time without functioning, secure maritime ports at home that facilitate the strategic sealift mission.

Additionally, maritime ports are vital assets to our communities. Waterborne commerce supports 28.5 million direct and indirect jobs across the United States. As a former mayor of Miami-Dade, home to the port of Miami, I understand personally how important ports can be to their local communities.
Maritime ports present soft targets to our adversaries, and large-scale operational disruptions at a major port could have a debilitating effect on our country. Therefore, it is critical that we understand and address the security vulnerabilities at our maritime ports.

This subcommittee has already begun work on this topic. Our subcommittee has engaged with DHS, the FBI, and the Department of Transportation to ensure resources are being appropriately allocated based on the evolving port threat landscape.

Last month the subcommittee heard from officials representing four different port authorities who discussed the challenges that their organizations are facing and opportunities to mitigate those challenges. Among the challenges we heard about from this panel was the alarming potential capabilities of nation-states, in particular the People’s Republic of China, and non-state actors to collect intelligence, steal sensitive data, and disrupt operations at our ports.

I'm especially concerned about the cranes and other equipment and technology in use at ports across the United States that are manufactured by the PRC state home entities and the opportunity for back-door access to sensitive port infrastructure. I have long advocated for Federal agencies with responsibilities for port cybersecurity to do more to address potential cybersecurity threats related to Chinese-made equipment and technology.

Last year I introduced legislation that limits the operation of foreign cranes and software at U.S. ports. We must remain vigilant in our fight against potential catastrophic events to our port infrastructure.

Today we are joined by leaders from the U.S. Coast Guard, the Cybersecurity and Infrastructure Security Agency, and the Transportation Security Administration, who are leading the Federal Government’s efforts to protect our Nation’s maritime ports. I look forward to discussing this important topic with our distinguished witnesses.

[The statement of Chairman Gimenez follows:]  

STATEMENT OF CHAIRMAN CARLOS A. GIMENEZ

MAY 10, 2023

This subcommittee’s hearing today will discuss security vulnerabilities at our Nation’s maritime ports. Ports are essential to our way of life in the United States. The United States is a maritime nation, with 361 commercial ports 25,000 miles of navigable channels, and 95,000 miles of shoreline. Maritime shipping is a critical component of our Nation’s economy. Approximately 90 percent of imports and exports enter and exit the United States by ship, generating over $4 trillion of economic activity each year.

Maritime ports are also essential to our military’s ability to respond to threats and project power overseas. During Operations Desert Shield and Desert Storm, the Navy’s Military Sealift Command delivered more than 12 million tons of equipment, vehicles, and materiel, facilitating the massive coalition force that ejected Saddam Hussein’s forces from Kuwait.

Our military cannot operate for sustained periods of time without functioning, secure maritime ports at home that facilitate the strategic sealift mission.

Additionally, maritime ports are vital assets to our communities. Waterborne commerce supports 28.5 million direct and indirect jobs across the United States.
As the former Mayor of Miami Dade, home to the Port of Miami, I understand personally how important ports can be to their local communities. Maritime ports present soft targets to our adversaries, and large-scale operational disruptions at a major port could have a debilitating effect on our country. Therefore, it is critical that we understand and address the security vulnerabilities of our maritime ports.

This subcommittee has already begun its work on this topic. Our subcommittee has engaged with DHS, the FBI, and the Department of Transportation to ensure resources are being appropriately allocated based on the evolving port threat landscape.

Last month, the subcommittee heard from officials representing four different port authorities who discussed the challenges their organizations are facing and opportunities to mitigate these challenges. Among the challenges we heard about from this panel was the alarming potential capabilities of nation-states—in particular the People’s Republic of China—and non-state actors to collect intelligence, steal sensitive data, and disrupt operations at our ports.

I am especially concerned about the cranes and other equipment and technology in use at ports across the United States that are manufactured by PRC state-owned entities and the opportunity for backdoor access to sensitive port infrastructure. I have long advocated for Federal agencies with responsibility for port cybersecurity to do more to address potential cybersecurity threats related to Chinese-made equipment and technology.

Last year, I introduced legislation that limits the operation of foreign cranes and software at U.S. ports. We must remain vigilant in our fight against potential catastrophic events to our port infrastructure.

Today, we are joined by leaders from the U.S Coast Guard, the Cybersecurity and Infrastructure Security Agency, and the Transportation Security Administration, who are leading the Federal Government’s efforts to protect our Nation’s maritime ports.

I look forward to discussing this important topic with our distinguished witnesses. I now recognize the Ranking Member, the gentleman from Michigan, Mr. Thanedar, for his opening statement.

Mr. Gimenez, I now recognize the Ranking Member, the gentleman from Michigan, Mr. Thanedar for his opening statement.

Mr. Thanedar. Thank you, Chairman Gimenez, for calling this important hearing. Thank you to our witnesses for joining us here today. Last month we had the opportunity to meet with port operators, including from the port of Detroit in my district, my home district, regarding the security of our Nation’s maritime ports. Today I’m eager to hear from our witnesses about how Federal agencies work together to protect our ports and safeguard the free flow of commerce.

More than 99 percent of America’s cargo from overseas arrives by maritime ports. That represents billions of dollars of goods moving through the port each and every day. It is vital for our national security and our economic future that we invest in protecting our sea ports from attacks.

American and foreign ports have been victims of cyber attacks that have halted the movement of goods and costs millions of dollars. Additionally, the COVID–19 pandemic led to many challenges for ports across the Nation, including staffing shortages, supply chain issues, and massive backlog of goods awaiting processing.

Today the maritime industry has made great progress to increase cyber protection and recover from backlogs, but more can be done. I’m eager to hear more about the Coast Guard and CISA’s efforts to expand cybersecurity measures at U.S. ports. Now is the time to invest in cyber readiness across essential transportation indus-
tries, as more cyber attacks on our ports and transportation systems could have devastating consequences.

I’m also interested to learn how the Coast Guard and TSA work together to administer the Transportation Worker Identification Credentials, or TWIC, program. Workers are the most valuable assets our ports have, and ensuring they can be vetted and receive credentials in a timely manner is critical to maintaining efficient and secure operations at our ports.

The U.S. Coast Guard, C–I–S–A—CISA, and TSA must work together to safeguard America’s maritime ports. We, in Congress, must support that mission and deliver the resources needed to invest in critical security advances.

I look forward to hearing from our witnesses today about what they need to carry out their mission effectively.

I thank the Chairman, and I yield back.

[The statement of Ranking Member Thanedar follows:]

STATEMENT OF RANKING MEMBER SHRI THANEDAR

MAY 10, 2023

Last month, we had the opportunity to meet with port operators, including from the Port of Detroit in my district, regarding the security of our Nation’s maritime ports. Today, I am eager to hear from our witnesses about how Federal agencies work together to protect our ports and safeguard the free flow of commerce. More than 99 percent of America’s cargo from overseas arrives by maritime port. That represents billions of dollars of goods moving through ports each and every day.

It is vital for our national security and our economic future that we invest in protecting our seaports from attacks. American and foreign ports have been victims of cyber attacks that have halted the movement of goods and cost millions of dollars. Additionally, the COVID–19 pandemic led to many challenges for ports across the Nation, including staffing shortages, supply chain issues, and massive backlogs of goods awaiting processing. Today, the maritime industry has made great progress to increase cyber protections and recover from backlogs. But more can be done.

I am eager to hear more about the Coast Guard and CISA’s efforts to expand cybersecurity measures at U.S. ports. Now is the time to invest in cyber readiness across essential transportation industries, as more cyber attacks on our ports and transportation systems could have devastating consequences.

I am also interested to learn how the Coast Guard and TSA work together to administer the Transportation Worker Identification Credential, or TWIC program. Workers are the most valuable assets our ports have, and ensuring they can be vetted and receive credentials in a timely manner is critical to maintaining efficient and secure operations at our ports.

The U.S. Coast Guard, CISA, and TSA must work together to safeguard America’s maritime ports. We in Congress must support that mission and deliver the resources needed to invest in critical security advances. I look forward to hearing from our witnesses today about what they need to carry out their missions effectively.

Mr. GIMENEZ. Thank you, Ranking Member Thanedar.

All 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

MAY 10, 2023

Seaports are key drivers of the U.S. economy and keeping them secure is vital to the American way of life. We must ensure that the Department of Homeland Security and its component agencies continue to secure U.S. ports against evolving threats, in coordination with port owners and operators and other stakeholders.

In 2018, activities at U.S. ports supported more than 31 million U.S. jobs and generated $5.4 trillion of total economic value, representing 26 percent of the Nation’s economy. As we saw during the COVID–19 pandemic, any disruptions or delays in
operations at ports are felt throughout society. Successful attacks against ports and the maritime transportation system can have ripple effects throughout our economy and drastic impacts to our national security. Indeed, we have seen the impact of such attacks in the past.

In 2018, for example, a cyber attack against Danish shipping company A.P. Moller-Maersk led to a shutdown of the Port of Los Angeles' largest cargo terminal along with several others around the world. The attack affected global shipping operations for weeks and cost Maersk as much as $300 million. Cyber threat actors continue to grow more sophisticated, and our security agencies must continue to work to stay a step ahead.

We must ensure the U.S. Coast Guard and the Cybersecurity and Infrastructure Security Agency are appropriately resourced and develop the necessary expertise to counter the latest cyber threats, including by issuing timely, actionable guidance and information to port owners and operators. The Coast Guard and CISA's efforts must be guided by a clear-eyed evaluation of the most pressing threats to the maritime industry based on the latest intelligence—not politics.

Additionally, DHS security programs must continue to prioritize the ability of ports to operate efficiently day in and day out. For example, the Transportation Security Administration must continue to evolve its processes for workers to obtain Transportation Worker Identification Credentials in a timely manner. Workers rely on obtaining TWIC cards for their livelihood, and delays in vetting and processing applications can have drastic impacts on not just individual workers but on ports that need to hire staff quickly in response to market demands. TSA's rollout last August of an option for TWIC holders to renew their cards on-line is a major step in the right direction.

The Department must continue to prioritize its efforts to protect the free flow of commerce through our Nation's ports given their significance to our national interest. I look forward to continuing this committee's oversight of DHS's port security efforts.

Mr. Gimenez. I am pleased to have the distinguished panel of witnesses before us today on this critical topic.

I ask that our witnesses please rise and raise their right hand.

[Witnesses sworn.]

Mr. Gimenez. You may be seated.

Let the record reflect that the witnesses responded in the affirmative.

Thank you again.

I would like—I would now like to formally introduce our witnesses.

Rear Admiral Wayne Arguin junior, currently serves as the assistant commandant for prevention policy with the United States Coast Guard. In this capacity, he's responsible for the development of national policy, standards, and programs promoting maritime security and safety.

Prior to his current assignment, Rear Admiral Arguin served as the director of inspection and compliance at Coast Guard Headquarters. His previous operational assignments include sector commander, Sector New Orleans. He also served as executive officer of Marine Safety Office Memphis, Tennessee and prevention department head at Sector Lower Mississippi River.

Mr. Eric Goldstein serves as the executive assistant director for cybersecurity with the Cybersecurity and Infrastructure Security Agency, CISA. In this role, Mr. Goldstein leads CISA's missions to protect and strengthen Federal civilian agencies and the Nation's critical infrastructure against cyber threats.

Previously, Mr. Goldstein was the head of cybersecurity policy, strategy, and regulation at Goldman Sachs where he led the firm's cybersecurity risk management program. From 2013 to 2017, Mr. Goldstein served at CISA's precursor agency, the National Protec-
tion and Programs Directorate, in various roles, including senior advisor to the assistant secretary for cybersecurity and senior counselor to the under secretary.

Mr. Neal Latta serves as the assistant administrator for enrollment services and vetting programs, ESVP, for the Transportation Security Administration. Mr. Latta leads ESVP in establishing and managing program operations, technology, budget, and end-to-end integration of TSA front-line vetting mission priorities.

Mr. Latta has over 25 years of Federal Government experience in implementing new program initiatives with the emphasis on biometrics and technology. Mr. Latta previously served as group chief of the screening and vetting group at the National Counterterrorism Center, where he oversaw and directed day-to-day operations for counterterrorism and high profile screening programs of all persons coming into the United States.

I want to thank all the witnesses for being here today.

I now 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, U.S. DEPARTMENT OF HOMELAND SECURITY

Admiral Arguin. Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee. I’m honored to be here today to discuss the top priority for the United States Coast Guard, protecting the Marine Transportation System, or MTS. I ask that my written testimony be entered into the record.

Mr. Gimenez. So done.

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 support $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 MTS is being shaped by three enduring drivers: First is the demand for increased capacity, from bigger ships and deeper channels to new industries harnessing our maritime advantage.

Second is the pressure to reduce the transportation’s environmental footprint and promote sustainability.

The only way that these meet—we meet these first two demands is the third driver: The introduction of new and complex technologies. We call these three drivers the triple challenge because together they create a far more complex operating environment.

The Coast Guard is uniquely positioned to face this triple challenge and manage risks in the MTS. At all times, we are a military service, a Federal law enforcement agency, a regulatory body, a sector risk management agency, a first responder, and a member of the U.S. intelligence community. We work across multiple levels of industry and government to assess security vulnerabilities with-
in the MTS, determine those risks, and development mitigation strategies.

This layered approach from the local to the international level is critical due to the size, diversity, and interconnectedness of the MTS.

Security assessments start with individual vessels and facilities. They are required by Federal regulation to conduct personalized security assessments, prepare an assessment report, and submit that report to the Coast Guard. We have boots on deck in the ports across the country conducting on-scene compliance activities, leading security exercises, and engaging with the port community.

At the regional level, area maritime security committees are comprised of Government and maritime industry leaders. Their collaborative development of an area maritime security plan ensures Government and industry security measures are coordinated to prevent and/or respond to a transportation security incident in our ports.

Above these regional efforts, we coordinate national-level activities. The relationships we maintain, the information we share, and the work we collaborate with across Government and industry is foundational to protecting the MTS.

Finally, our efforts to secure the MTS extend overseas. We conduct in-country foreign port assessments and apply international maritime organization standards to assess the effectiveness of security and antiterrorism measures in foreign ports and on foreign ships in our ports.

To support the whole-of-government effort, we apply our proven prevention and response framework to prevent or minimize disruptions to the MTS in ports around the country. Our authorities and capabilities cut across threat vectors, allowing operational commanders at the port level to quickly evaluate risks, apply resources, and lead coordinated Federal responses to all hazards. We also recognize that threats to the MTS constantly change and that we must continually evolve as a service and collaborate with our partners to address emergent needs.

Protecting MTS is a top priority for the Coast Guard, and I recognize it is also a top priority for this Congress. We are grateful for the recent appropriations that help us safeguard the MTS, and especially from threats in the cyber domain. We will maximize the return on this critical investment.

I welcome your questions on the vital work the Coast Guard does every day to help 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 prepared statement of Admiral Arguin follows:]

PREPARED STATEMENT OF REAR ADMIRAL WAYNE R. ARGUIN

10 May 2023

INTRODUCTION

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee. I am 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 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 a member of the U.S. intelligence
community. We are uniquely positioned to ensure the safety, security, and stewardship of the maritime domain.

Since the early days of the Revenue Cutter Service, we have 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 cyberspace—our ethos and operational doctrine remain steadfast. We employ a risk-based approach to protect the Nation from threats in the maritime environment. 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. The MTS' complexity and consequence to the Nation cannot be overstated. It is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports. 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 accounts for the employment of more than 30 million Americans. It protects critical national security sealift capabilities, enabling U.S. Armed Forces to project and maintain power around the globe. We remain laser-focused on the safety and security of the MTS as an economic engine and strategic imperative, and we continue to serve as the Sentinels envisioned at our founding.

EVALUATING VULNERABILITIES—A SHARED RESPONSIBILITY

Safeguarding the MTS requires diligent assessment and remediation of vulnerabilities. The Coast Guard works across multiple levels of industry and government 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, diversity, and interconnectedness of the MTS.

Locally: Vessel and Facility Security Assessments

Security assessments in U.S. ports and waterways start with individual vessels, port facilities, and outer continental shelf facilities. The Maritime Transportation Security Act (MTSA) regulations in 33 CFR 104, 105, and 106 place specific requirements on regulated entities to conduct personalized security assessments, analyze the results, and prepare a security assessment report that is included in their security plans.

A completed security assessment report must be submitted to the Coast Guard as part of the plan approval process and include a description of how the on-scene survey was conducted, key facility operations to protect, each vulnerability found, security measures to address each vulnerability, and potential gaps in security policies and procedures.

In February 2020, the Coast Guard provided further guidance to the regulated industry on incorporating computer systems and networks into their required assessments and plans. During inspections to verify compliance, the industry sought more specific guidance on ways to integrate cyber into their existing security regime. The Coast Guard partnered with the Homeland Security Systems Engineering and Development Institute, a Federally-funded research and development center operated by the MITRE Corporation, and the National Maritime Security Advisory Committee (a Federal Advisory Committee) to develop the Maritime Cybersecurity Assessment and Annex Guide. This guide was released in January 2023 and provides a clear process for identifying and describing cybersecurity vulnerabilities, then addressing those vulnerabilities in mandated security plans.

For foreign ships operating in U.S. waters, the process is very similar to MTSA-regulated vessels and facilities. Per the International Ship and Port Facility Security Code (ISPS Code), each ship must conduct a Ship Security Assessment that identifies key shipboard operations to protect; threats to key shipboard operations; 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, and is verified by the Coast Guard during regular compliance examinations in U.S. ports.

Regionally: Area Maritime Security Assessments and Plans

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

The AMSC’s 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, and recover from a threatened or actual Transportation Security Incident (TSI).

The COTP/FMSC and the AMSC ensure that a formal AMS Assessment for their entire Area of Responsibility (AOR) is conducted at least every 5 years. The AMS Assessment must also be evaluated at least annually to ensure its adequacy, accuracy, and consistency.

Nationally: Interagency Coordination and Assessment

As outlined in Presidential Policy Directive 21, along with the Department of Transportation, the Coast Guard is the co-Sector Risk Management Agency (SRMA) for the Maritime Transportation Subsector. As a SRMA, the Coast Guard is responsible for coordinating risk management efforts with the Cybersecurity and Infrastructure Security Agency (CISA), other Federal departments and agencies, and MTS stakeholders.

CISA is a key partner in all our risk management activities. CISA’s technical expertise directly supports the 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. The relationship with CISA is strong and will continue to mature.

As a member of the U.S. intelligence community, the Coast Guard provides unique authorities, opportunities, and capabilities to collect, fuse, analyze, and share information and intelligence across domestic and international government and non-government stakeholders throughout the MTS. The Coast Guard’s intelligence authorities allow for a collective understanding of factors and entities affecting the maritime domain, including physical security and cybersecurity. Threats, such as ransomware attacks, continue to mature in effectiveness and prevalence, requiring the intelligence community to align resources and integrate efforts that protect the safety and security of the MTS.

The 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 Coast Guard and DoD ensures the Nation’s surge capability and sea lines of communication will be secure and available during times of crisis. By sharing threat intelligence, developing interoperable capabilities, and using DoD’s expertise, the Coast Guard enables national security sealift capabilities and jointly supports our Nation’s ability to project power around the globe.

The Coast Guard serves as a partner to the Federal Emergency Management Agency (FEMA) in the Port Security Grant Program (PSGP) by providing subject-matter expertise in maritime security. FEMA is responsible for the administration and management of the program, which includes designing and operating the administrative mechanisms and managing the distribution and tracking of funds. The PSGP is designed to support AMSPs and facility security plans (FSPs) to protect critical port infrastructure from terrorism. All U.S. ports are eligible for PSGP funding. PSGP funds are intended to offset the costs for maritime security risk mitigation projects borne by maritime partners. To date (fiscal year 2002–fiscal year 2022), the PSGP distributed over $3.73 billion to port stakeholders to make security improvements, including assisting facilities with capital investments for MTSA compliance.

Internationally: International Port Security Program

Coast Guard efforts to secure the MTS also extend overseas. By leveraging international partnerships, and through the Coast Guard International Port Security (IPS) program, the Coast Guard conducts in-country foreign port assessments and applies the International Maritime Organization’s (IMO) International Ship and
Port Facility Security (ISPS) Code to assess the effectiveness of security and anti-terrorism measures in foreign ports. If the Coast Guard finds that a country's ports do not have effective security and anti-terrorism measures, we may impose Conditions of Entry (COE) that define additional security measures that vessels arriving to the United States from those ports must implement. COE may result in security verifications of vessels before they enter U.S. ports to verify that additional security measures were taken in foreign ports. The IPS program also conducts capacity building engagements to assist countries in implementing effective anti-terrorism measures.

THE U.S. COAST GUARD'S APPROACH

The U.S. Coast Guard's approach to support the whole-of-Government effort, the Coast Guard applies a proven prevention and response framework to prevent or mitigate disruption to the MTS from the many risks it faces. Coast Guard authorities and capabilities cut across threat vectors, allowing operational commanders at the port level to quickly evaluate risks, apply resources, and lead a coordinated and effective response.

Prevention
The Prevention Concept of Operations—Standards, Compliance, and Assessment—guides all prevention missions. 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, compliance activities systematically verify that 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.

Importantly, the Coast Guard operationalizes this framework at the port level. Coast Guard COTPs oversee MTSA-regulated vessels and facilities through their mandated Vessel or Facility Security Assessments and Plans. These plans set baseline activities to protect the MTS through personnel training, drills and exercises, communication, vessel interfaces, security systems, access control, cargo handling, delivery of stores, and restricted area monitoring.

The Coast Guard also has Port Security Specialists and MTS Cybersecurity Specialists in each Captain of the Port Zone. These new positions create a dedicated staff to build and maintain port-level security-related relationships, facilitate information sharing across industry and Government, advise Coast Guard and Unified Command decision makers, and plan security exercises.

Response
Similar to the Prevention Concept of Operations, the Coast Guard has a proven, scalable response framework that can be tailored for all hazards. This is especially important as cyber incidents can quickly transition to producing physical impact, requiring operational commanders to immediately deploy assets to mitigate risks. Depending on the incident's size and severity, commanders will set clear response priorities, request specialized resources to help mitigate risk, and notify interagency partners to help coordinate the response. The Service is not approaching this alone.

By regulation, MTSA-regulated vessels and facilities are required to report TSIs, breaches of security, and suspicious activity without delay. These reports enable operational commanders to rapidly notify other Government agencies, evaluate associated risks, deploy resources, and unify the response.

For complex responses, the Coast Guard maintains deployable teams with specialized capabilities that can support operational commanders across a spectrum of prevention and response needs. These teams include specially-trained law enforcement teams that can bolster physical security, pollution response teams for significant oil spills or hazardous material releases, and cyber protection teams that can help local responders navigate the highly technical aspects of cyber incident assessment and response.

Through both prevention and response activities in the field, and engagements with industry, the Coast Guard captures lessons learned, recommendations, and best practices that strengthen the maritime industry's security posture and inform future policy, law, and regulations.

FUTURE FOCUS

Working in close collaboration with CISA and other Government partners, foreign allies, and industry, the Coast Guard will continue to leverage strong and estab-
lished relationships across the maritime industry—at all levels—to assess and ad-
dress security vulnerabilities.

The Coast Guard has secured and safeguarded the maritime environment for over
230 years and, during that time, has faced many complex challenges. We have
honored our operating concepts, bolstered our capabilities, and strengthened our re-
solve. These same concepts and capabilities will secure and protect the Nation and
maritime critical infrastructure from malicious activity in all domains. In address-
ning risks to ports and other components of the MTS, the Coast Guard's commitment
is to address those risks with the same level of professionalism, efficiency, and effec-
tiveness that the public has come to expect.

Thank you for the opportunity to testify today and thank you for your continued
support of the United States Coast Guard. I am pleased to answer your questions.

Mr. Gimenez. Thank you, Rear Admiral Arguin.

I now recognize Executive Assistant Director Goldstein for 5 min-
utes to summarize his opening statement.

STATEMENT OF ERIC GOLDSMITH, EXECUTIVE ASSISTANT DI-
RECTOR, CYBERSECURITY AND INFRASTRUCTURE SECU-
RITY AGENCY, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. Goldsmith. Chairman Gimenez, Ranking Member Thanedar,
Members of the subcommittee, thank you for the privilege of joining
today to speak about such a critical issue, securing our Marine-
time Transportation System, or MTS.

At CISA, we work every day to understand, manage, and reduce
risk to our Nation’s critical infrastructure; and given the com-
plexity of the MTS, we do so in deep partnership with our partners
at Coast Guard and TSA and, most importantly, with the owners
and operators of critical infrastructure across the country, includ-
ing the operators of our Nation’s ports.

We are acutely concerned by the risk of Chinese cyber aggression
targeting our Nation’s critical infrastructure. It is that focus that
catalyzes our priority and that drives our investment in this crit-
ical area.

We’re focused on reducing risk in the country in partnership with
Coast Guard and TSA in several ways. First, we focus on providing
actionable information that the owners and operators of critical in-
frastucture can use to reduce their risk in a timely way. We often
joint seal cybersecurity publications with our partners at the Coast
Guard to provide unity of effort, unity of communication across the
Government so that owners and operators understand the risk and
take action in response.

We undertake exercises to ensure that we have tested our proc-
esses as a Government and a cyber community, including our na-
tional-scale cyber storm exercise in which Coast Guard and TSA
are both core participants. We coordinate and convene, including to
the maritime sector Government Coordinating Council, which
brings together partners in Government and the private sector to
identify shared risks, and derive shared solutions to reduce risks
across the country.

But we’re also focused on immediate and near-term risk reduc-
tion. Every year CISA and our partners at the NSA produce a pub-
lication with the cybersecurity vulnerabilities most frequently ex-
loited by Chinese cyber actors. We then scan thousands of organi-
zations across critical infrastructure, including in the maritime sec-
tor, to identify the prevalence of vulnerabilities on their network;
and we have over 100 regional personnel who every day are working with organizations to help them mitigate vulnerabilities.

We're also focused on reducing risks in the supply chain, particularly to high-risk devices manufactured by China-based organizations. We are currently focused on devices on the Federal Communications Commission's high-risk list. We've identified nearly 100 organizations across critical sectors that we can see are running these kinds of high-risk devices, and our regional personnel are working with these organizations to get them to modernize and upgrade their equipment so they are no longer running devices that could pose inordinate risk to their critical networks.

We also have programs like CyberSentry, which provides Government sensors to detect threats on some of the highest-risk private networks and our pre-ransomware notification initiative where we identify ransomware intrusions that have occurred but where harm hasn't yet happened, where there hasn't yet been an encryption event, and notifying those victims to mitigate before damage happens.

But we also recognize that we need to focus on strategic change, even as we focus on tactical risk reduction efforts, and so we're also focused on long-term cyber defense planning with partners like Coast Guard and TSA to understand the most significant cybersecurity risks facing our country and bringing together partners to plan, exercise, and execute in ways that reduce risk over time and also recognizing that the most scalable cybersecurity solution is using technology products that are safe and secure by design and default wherever they're deployed.

So we work with major technology companies to ensure that, whether it is a port or a hospital or water utility, they are using technology that is as hardened as possible against the threat that we know we’re facing.

This threat is significant. We have tremendous work to do as a Nation, as a community, but the agencies at this table and across Government are working every day, diligently, to make sure that we are staying ahead of the threat as it evolves.

Thank you again for the chance to appear. I look forward to your questions.

[The prepared statement of Mr. Goldstein follows:]

PREPARED STATEMENT OF ERIC GOLDSTEIN

MAY 10, 2023

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

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

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

PARTNERSHIP WITH THE UNITED STATES COAST GUARD AND THE TRANSPORTATION SECURITY ADMINISTRATION

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

First, we must provide members of the maritime community, including port operators, with actionable information to protect their systems. For this reason, CISA and the Coast Guard frequently engage in joint amplification or development of combined products for this community, with recent examples including CISA’s amplification of a Coast Guard Safety Alert with recommended cybersecurity best practices for commercial vessels and a joint advisory regarding malware exploiting the Log4Shell vulnerability. In addition, the Coast Guard was a key partner in our development of the Cross-Sector Cybersecurity Performance Goals (CPGs), which provide a straightforward and actionable set of cybersecurity actions prioritized by cost, impact, and complexity and organized around the National Institute of Standards and Technology Cybersecurity Framework. The CPGs are a foundational tool to help any organization align limited cybersecurity resources toward the most impactful investments. We look forward to partnering closely with the Coast Guard to develop sector-specific goals for maritime stakeholders that reflect the unique technology and risk considerations of the sub-sector.

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

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

SUPPORTING OUR PARTNERS TO ACTIVELY REDUCE RISK

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

As a key part of this effort, we enable network owners and operators to harden their networks against known and potential tactics, techniques, and procedures used by PRC cyber actors. For example, we published in late 2022 a joint advisory with the National Security Agency and the Federal Bureau of Investigation outlining the
vulnerabilities most frequently used by PRC actors, enabling organizations around the country to close down intrusion paths commonly used by the PRC to achieve their strategic goals. We regularly scan over 5,000 Federal, critical infrastructure, and State, local, Tribal, and territorial (SLTT) partners’ networks upon their request to identify the presence of these vulnerabilities and notify identified entities to prioritize urgent mitigation. More recently, we have undertaken an effort intended to make network owners and operators aware of the prevalence of devices produced by PRC-based vendors that are listed on the Federal Communications Commission’s “Covered List,” which, under the Secure and Trusted Communications Networks Act of 2021, pose an “unacceptable risk to the national security of the United States or the security and safety of United States persons.” Using commercial tools, we have identified such products used on critical infrastructure networks across the country and have already notified 88 critical infrastructure organizations using such products about the potential associated risks. In nearly all cases, the notified entities have chosen to take urgent steps to replace these products from their networks and reduce the likelihood of unauthorized access by PRC actors.

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

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

Looking to the future, CISA is continuously developing new capabilities to help our stakeholders drive down cyber risk based upon their feedback and needs. We are looking forward to several impactful new efforts in the coming months, including an effort that will expand one of our cybersecurity shared service offerings beyond the Federal sphere to certain critical infrastructure entities, a new attack surface management service, and a modernized cyber threat intelligence service. Through each of these efforts, we will work closely with the maritime community to understand their needs and maximize our ability to deliver services, information, and guidance that helps our partners detect, prevent, and effectively respond to cyber risks.

GETTING AHEAD OF THE THREAT

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

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

CONCLUSION

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

Mr. Gimenez. Thank you, Mr. Goldstein.

I now recognize Assistant Administrator Latta for 5 minutes to summarize his opening statement.

STATEMENT OF JOHN “NEAL” LATTA, ASSISTANT ADMINISTRATOR, ENROLLMENT SERVICES AND VETTING PROGRAMS, TRANSPORTATION SECURITY ADMINISTRATION, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. Latta. Good afternoon, Chairman Gimenez and Ranking Member Thanedar and distinguished Members of the subcommittee. Thank you for inviting me to testify on port security, specifically the Transportation Security Administration's role in vetting maritime transportation workers for the Transportation Worker Identification Credential, or TWIC, Program.

TSA is committed to securing the Maritime Transportation System, including waterways, ports, and land-side connections, against evolving and emerging risks. TSA partners with public and private-sector stakeholders, such as the U.S. Coast Guard, U.S. Customs and Border Protection, port owners and operators, and national trade and labor associations, to secure the Maritime Transportation System from potential security threats.

TSA's Enrollment Services and Vetting Program Office administers TSA's enrollment, vetting, and credentialing programs. This includes end-to-end program management and oversight of the technology, operations, and resources that support TSA's security threat assessment, known as the STA.

These programs—these vetting programs are the foundation for identifying potential threats to U.S. critical infrastructure specific to maritime security. TSA vets over 2.2 million maritime transportation workers, such as longshoremen, merchant mariners, truck drivers, engineers, and individuals in other occupations who require a TSA—a TWIC STA for access to secure areas of port facilities and vessels.

Since the TWIC program was established in 2007, TSA has enrolled over 7 million transportation workers. The TWIC program is a fee-based DHS security program mandated by the Maritime Transportation Security Act of 2002, or MTSA. TWIC, jointly administered by TSA and the U.S. Coast Guard, is one of several layered security measures incorporated by Federal, State, and local
partners to prevent potential security breaches and incidents targeting U.S. critical and maritime infrastructure.

TSA is responsible for enrolling and vetting applicants, adjudicating the STA, and issuing the biometric credential or TWIC card. The U.S. Coast Guard administers the security program and TWIC access control standards for the facility and vessel owners and operators to implement.

Facility and vessel operators determine who is authorized to access secure areas of the MTSA-regulated facilities or vessels and verify that each individual holds a valid TWIC. Authorized access requires three functions to be performed: Verification that the individual has undergone the STA, verification that the individual is who they say they are, verification that the individual is eligible to access a specific area.

TSA and its enrollment provider oversees more than 570 enrollment centers Nation-wide, including all 50 States, the District of Columbia, and the U.S. territories. Following the collection of biometric fingerprints and facial photograph and biographic information, TSA performs the vetting of TWIC applicants for criminal history, intelligence or ties to terrorism, and lawful presence.

TSA adjudicates most TWIC applicants, approximately 60 percent of enrollments, within 24 hours, and applicants receive their TWIC card via the mail within 7 to 10 business days. Approximately 40 percent of the enrollments are considered complex cases due to a potential disqualifying factor.

Processing these cases may take TSA up to 30 to 60 days to make a determination. While most of these cases will ultimately result in the applicant receiving a TWIC, some applicants will be notified that they have potentially disqualified. All TWIC applicants are afforded an opportunity to participate in the TSA redress process, which allows individuals to appeal TSA's initial decision or request a waiver.

Customer service and engagement are critical success factors for TSA's TWIC program. TSA recognizes its need to be efficient for transportation worker population to be able to perform their job. TSA has acknowledged the vital role a TWIC holder serves in supporting the flow of commerce.

The TWIC program is focused on enhancing its security value while reducing the burden of obtaining and renewing a TWIC. Already, TSA has implemented programs to reduce the amount of time applicants spend at enrollment centers, making renewing easier, and reduced TWIC costs for on-line applicants.

TSA continues to work to improve the enhanced maritime security through its TWIC program.

Chairman Gimenez, Ranking Member Thanedar, and Members of the subcommittee, thank you for the opportunity to appear before you today. I look forward to your questions.

[The prepared statement of Mr. Latta follows:]

PREPARED STATEMENT OF JOHN “NEAL” LATTA

MAY 10, 2023

Good afternoon, Chairman Gimenez, Ranking Member Thanedar, and distinguished Members of the subcommittee. Thank you for inviting me to testify on port security, specifically the Transportation Security Administration’s (TSA) role in vet-
ting maritime transportation workers for the Transportation Worker Identification Credential (TWIC) program. My testimony will highlight TSA’s security responsibilities and achievements in the maritime environment and how TSA is working to enhance transportation security while bolstering customer service and supporting the flow of commerce.

TSA’S ROLE IN SECURING THE MARITIME ENVIRONMENT

TSA is committed to securing the Maritime Transportation System (MTS), including waterways, ports, and land-side connections, against evolving and emerging risks, such as physical and cyber intrusions. TSA partners with public and private-sector stakeholders, such as U.S. Coast Guard (USCG), U.S. Customs and Border Protection (CBP), port owners and operators, and national trade and labor associations, to secure the MTS from potential security threats.

TSA’s Enrollment Services and Vetting Programs (ESVP) office administers TSA’s enrollment, vetting, and credentialing programs, including the end-to-end program management and oversight of the technology, operations, and resources that support TSA’s Security Threat Assessment (STA) programs. The TWIC program is an STA program designed to mitigate insider threats. These vetting programs are the foundation for identifying potential threats to U.S. critical infrastructure, and TSA prioritizes the vetting and adjudication of its worker populations to minimize impediments to the economy, industry, and the workforce. Specific to maritime security, TSA vets over 2.2 million maritime transportation workers, such as longshoremen, merchant mariners, truck drivers, engineers, and individuals in other occupations who require a TWIC STA for access to secure areas of port facilities and vessels.

TWIC OVERVIEW

The TWIC program is a fee-based Department of Homeland Security (DHS) security program mandated by the Maritime Transportation Security Act of 2002 (MTSA), which mandates that individuals requiring unescorted access to MTSA-regulated facilities and vessels must be issued a biometric transportation security card once the individual is determined not to pose a risk to transportation or national security. TWIC, jointly administered by TSA and USCG, is one of several layered security measures incorporated by Federal, State, and local partners to prevent potential security breaches and incidents targeting U.S. critical and maritime infrastructure. Since the TWIC program was established in 2007, TSA has enrolled over 7 million transportation workers.

TWIC AND THE SECURITY THREAT ASSESSMENT PROCESS

TSA is responsible for enrolling and vetting applicants, adjudicating the STA, and issuing the biometric credential. The USCG administers the security program and TWIC access control standards for facility and vessel owners and operators to implement. Facility and vessel operators determine who is authorized to access secure areas of their MTSA-regulated facilities or vessels and verify that each individual holds a valid TWIC. Authorized access requires three functions to be performed: verification that an individual has undergone an STA, identity management, and establishment of the individual’s business purpose.

TSA and its enrollment provider oversee more than 570 enrollment centers nationwide, including all 50 States, the District of Columbia, and U.S. territories. Following the collection of biometric (i.e., fingerprints and facial photograph) and biographic information, TSA creates a TWIC record in its case management system and performs the vetting of applicants for criminal history, intelligence/ties to terrorism, and lawful presence. Based on the vetting results, TSA adjudicates the case based on the interim and permanent disqualifying factors listed in TSA’s regulations in 49 CFR Part 1572.

TSA’s case management system adjudicates most TWIC applicants—approximately 60 percent of total enrollments—within 24 hours and an applicant receives their TWIC card via mail within 7 to 10 business days. Approximately 40 percent of enrollments are considered complex cases due to a potentially disqualifying factor. Processing these cases may take TSA up to 30 to 60 days to make a determination. While most of these cases will ultimately result in the applicant receiving a TWIC, some applicants will be notified that they have been potentially disqualified. All TWIC applicants are afforded an opportunity to participate in the TSA redress process, which allows individuals to appeal TSA’s initial decision or request a waiver.
TWIC CONTRIBUTIONS TO THE MOVEMENT OF COMMERCE

TSA mitigates security risks to maritime transportation by recurrently vetting TWIC holders to ensure individuals who pose a potential threat to transportation and national security cannot access secure areas. TSA continually strives to enhance its identity management and vetting capabilities. For example, in 2021, TSA began subscribing all new TWIC holders in Federal Bureau of Investigation Rap Back Services. This automation provides TSA with more accurate and real-time information on TWIC holder criminal activities after enrollment.

To facilitate the movement commerce, TSA has partnered with supply chain and maritime stakeholders to alleviate potential bottlenecks where TWIC or other TSA vetting programs could impede such movement. For example, in 2021, DHS and TSA contributed to the White House Supply Chain Disruptions Task Force and met with representatives at the Ports of Los Angeles and Long Beach, California, to discuss strategies to support essential workers accessing port terminals. TSA took immediate steps to address the needs of its maritime partners, including expanding enrollment center operations, expediting the vetting of mission-critical transportation workers, and reducing the time and burden associated with obtaining a TWIC.

CUSTOMER EXPERIENCE

Customer service and engagement are critical success factors for TSA’s STA programs. TSA recognizes transportation worker populations require efficient services from TSA to obtain and retain certifications, occupations, and professions. TSA is focused on enhancing the security value of its program while reducing the burden of obtaining a TWIC.

In 2009, TSA implemented TWIC One Visit which enables eligible workers to receive their TWIC card at a designated address instead of returning to an enrollment center for pick-up and activation. Today, 91 percent of total TWIC applicants receive their card via mail. In August 2022, TSA implemented a new on-line renewal capability for most TWIC applicants who maintain or previously maintained an active TWIC STA. Approximately 54 percent of active TWIC cardholders enroll for a new TWIC after their STA expires 5 years from the date of issuance. Of those workers renewing a TWIC, nearly 80 percent are using TSA’s on-line renewal capability, thereby eliminating the cost and time burden associated with traveling to a physical enrollment center. TWIC One Visit and on-line renewal grant maritime workers their TWICs faster, allowing them to fulfill their roles in transportation security more expediently.

In addition, due to the reduced costs associated with the on-line transaction, TWIC applicants now pay a reduced fee when renewing their credentials on-line: $117.25, compared to the in-person fee of $125.25. Since TSA issued the first TWIC in October 2007, TSA has not increased the enrollment fee for TWIC applicants.

CONCLUSION

TSA continues to work to improve and enhance maritime security through its TWIC program. Chairman Gimenez, Ranking Member Thanedar, and Members of the subcommittee, thank you for the opportunity to appear before you today. I look forward to your questions.

Mr. Gimenez. Thank you, Mr. Latta.

Members will be recognized by order of seniority for their 5 minutes of questioning.

I now recognize myself for 5 minutes.

Rear Admiral Arguin, over the past few years, I have continued to raise concerns about the wide-spread presence of Chinese manufactured cranes in our Nation’s ports. I’m particularly concerned about the use of Chinese technology and equipment, as well as the ports’ industries overreliance on Chinese cranes.

On April 3, I joined several of my colleagues in sending a letter to DHS asking about their efforts to address the vulnerabilities related to these cranes. DHS has yet to respond.

Can you explain what security measures the Coast Guard has in place to evaluate foreign manufactured equipment and software in use at our ports? These can include cybersecurity assessments,
penetration testing, configuration review, or malware vulnerability assessments.

Admiral Arguin. Mr. Chairman, so the Coast Guard’s role in ensuring port security from the local level, the local sector commander, captain of the port, uses its maritime security specialist to engage those entities that have ZPMC cranes. At that local level, they have had conversations about potential vulnerabilities identified with our partnership with CISA.

We’ve also engaged our cyber protection team, elements of our Coast Guard cyber command to perform voluntary assessments of those networks to understand, better understand the vulnerabilities associated with those systems, as well as systems throughout the ports.

At the regional level, the Area Maritime Security Committee had—we’ve had conversations with each of those entities to ensure they understand the potential vulnerabilities and the likelihood of a potential disruption.

At the national level, I’ve had similar conversations with leadership, with port authorities around the country to make sure, A, they’re aware of the potential vulnerabilities and to get a better understanding of the potential impacts that those vulnerabilities may have.

Mr. Gimenez. Do we have laws in place that actually hinder ports from not buying these cranes?

Admiral Arguin. Mr. Chairman, I’m not aware of the specifics on purchasing particular equipment. I am certainly interested in understanding those networks and who has access to those networks to better understand the potential impacts on commerce.

Mr. Gimenez. OK.

Switching gears a little bit, during the week of February 27, 2023, the Coast Guard, working with the State Department, scheduled facility visits for a Cuban delegation that included members of the Cuban border guard and the Cuban Ministry of Interior. This visit would have included a tour of the Coast Guard headquarters here in Washington, DC.

After my colleagues and I raised concerns with this visit, the Coast Guard canceled the headquarters portion of the unit tour but continued with the rest of the scheduled activity.

As early as January 2021, Global Magnitsky sanctions were placed on the Cuban Ministry of Interior for its complicity in serious human rights abuses in Cuba. Individuals from the same Cuban ministry were invited to tour our Coast Guard headquarters.

According to DHS, in September—in December 2022, the Office of Foreign Assets Control in the Treasury Department put into place a new general license for the Global Magnitsky program that authorizes all transactions otherwise prohibited, provided that they are for official U.S. Government business.

Can you confirm whether the Coast Guard received a license to invite members of Cuba’s Ministry of Interior, a sanctioned entity, to tour their headquarters? Has the Coast Guard requested additional licenses for foreign delegation visits since then?
Admiral ARGUIN. Mr. Chairman, I will have to get back to you on whether or not we received any specific licensing for foreign visits to other country's headquarters.

The International Port Security Program is a vital opportunity for us to evaluate foreign ports, ships that call on those foreign ports before they get to the United States. That reciprocity that we've established to ensure that international standards are being applied uniformly and then evaluated so that best practices could be shared is an important aspect of the layered approach that the Coast Guard takes.

Mr. GIMENEZ. Do you think that the Cuba is a friendly nation to the United States?

Admiral ARGUIN. Mr. Chairman, the Coast Guard's responsibility for ensuring port security and ensuring the international norms that have been established under IMO requires us to ensure that we have reciprocity on those ports that have interest for the Coast Guard. If there are—if ships call on those ports and intend to call on U.S. ports, we want to better understand what that—the security measures that are in place in those ports so that we can effectively evaluate security in our own ports.

Mr. GIMENEZ. Thank you.

I yield back.

I'll recognize the Ranking Member from Michigan, Mr. Thanedar.

Mr. THANEDAR. Thank you, Mr. Chairman.

I think I want to start with the concern the Chairman expressed in his questions, so—regarding, you know, reciprocal port visits by the United States to the foreign ports, as well as allowing others to visit our ports.

Rear Admiral, my question is: What is the value of maintaining access to foreign ports to carry out security assessments? What would be the consequences if we start refusing reciprocal visits, like some Members across the aisle have suggested, if we stop these visits by others and reciprocally if we are not allowed to visit these foreign ports?

Second, can these visits happen and yet we can protect our sensitive information? Because nobody wants, you know, our sensitive information to fall in the wrong hands. At the same time, we need these reciprocal inspections for our own safeguards. How can this be done? Can this be done without—by still securing the sensitive information?

Admiral ARGUIN. Ranking Member Thanedar, the importance of the International Port Security Program and its reciprocal visit program really does two things for us. One, it is—it demonstrates the Coast Guard's leadership role in international—establishing and reinforcing international norms for port security. That's required under the international port security protocols.

The availability of us or our teams to be able to go into a foreign port, assess the security protocols that are in place, provides us with visibility on potential implications or vulnerabilities that may be on ships that would call on U.S. ports. So it gives us advance notification, and it gives us the opportunity to put additional safeguards in place for those vessels where we would not have that same visibility.
It also allows us to share best practices so that those ships that are calling on our ports and the countries that are working with us to ensure that we are all raising the standard, we all—elevate the protective measures that are in place to prevent bad things from happening within our ports.

Mr. THANEDAR. So it would be irresponsible for us to stop this bilateral inspections of each other’s ports.

Admiral ARGUIN. Ranking Member, I think that it would not afford us an opportunity to learn from others but also then help others elevate their standards for security. It would have the potential implication of us requiring additional safeguards in place that may have an impact on the safe and efficient movement of cargos within the United States.

Mr. THANEDAR. Do you believe there is a way for you to safeguard our sensitive information while these visits are taking place?

Admiral ARGUIN. Yes, sir. I think the reciprocal visit really is talking about best practices. It does not get into sensitive information. It talks about, are there best ways to ensure fence line, physical security, and others? Yes, sir, I think we can preserve sensitive information.

Mr. THANEDAR. Thank you.

Mr. Latta, again, thank you for being here.

Many of the workers, including many port workers, truck drivers in my district rely on the TWIC card for their livelihood, and I wanted to know what has been done, what TSA has been doing in safeguarding and making sure that these TWIC cards are processed and accessible to the workers as early as—as soon as possible.

Mr. Rear Admiral, my question again is that Coast Guard has delayed full implementation of the electronic TWIC and biometric readers at ports for several years, and I’m wondering, how are we going to implement the requirements of Safe Port Act of 2006?

Mr. LATTA. Thank you for that question.

We take very seriously the adjudication processing time frames for the TWIC card. We have put some technology in place to really speed that up, and, for the most part, as I said in my testimony, 60 percent of individuals get their TWIC card in 7 to 10 business days.

We also, as of August of last year, we have implemented now online renewal. So there’s no longer a need to come into an enrollment center to do your enrollment for your renewal of your card. So we’re finding 80 percent of our applicants are going through that process.

So we have done a lot to move there. We’ve also hired additional adjudicators and put technology there to also speed up that process.

Mr. THANEDAR. Thank you.

Mr. GIMENEZ. The gentleman’s time has expired.

I now recognize the gentleman from Louisiana, Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman.

Mr. Latta, not to beat that subject, can my staff exchange contact data with your staff so that we can communicate directly regarding delays for trusted traveler applications and TWIC cards, et cetera?
You answered the question very well, but can we—can our staff exchange data? OK, we’ll do that at this hearing.

Mr. LATTA. Yes, sir.

Mr. HIGGINS. Admiral Arguin, I have a couple of questions for you, sir, and I’m going to touch on something. In the 2017 and 2018 time frame in south Louisiana, we had reports of a gentleman in a Coast Guard jacket duck hunting in a kayak. Would that have been you? Potentially, that’s you, sir. We may have further questions for you on that topic.

So, on security for our ports, it’s really an evolving challenge, and we have to stay ahead of some of these threats, and the heightened awareness is, I believe, the beginning of—as they say, chance favors the prepared mind.

We were made aware of a particular threat in south Louisiana recently. Two men from New York city of Russian nationals, Russian descent, rented a car in Miami, were arrested in south Louisiana flying very advanced drone systems over a chemical plant, and that investigation was initiated by the St. Charles Parish Sheriff’s Office.

They had very advanced technologies with them, and they were arrested. The investigation revealed that that drone had flown extensively over two other chemical plants prior to their arrest, which was the third chemical plant. They—their bond was set that the judge thought was high. It was 100 grand. They posted the bond, and they’re gone. February. The FBI is working on the case, but the point is this threat is out there.

So Admiral—and Mr. Goldstein may have something to adhere, and I’m happy to yield my remaining couple minutes of time. It’s important to answer. What is the Coast Guard doing to work with your colleagues at CISA and FBI at the Federal level and working in close relation with local law enforcement? What is the Coast Guard doing to secure our ports against the next generation of threat, including like the one I just described?

I yield.

Admiral ARGUIN. Congressman, at the local level, the sector commander, captain of the port, engages with local port partners, parish law enforcement, and their regional coordinating mechanism through either their FBI or other law enforcement entities. Clearly, any anomalous activity, whether it’s an unmanned system or somebody that may be just not doing things that we think are appropriate around a critical infrastructure, that information needs to get to us, to law enforcement in a fast way so that we can investigate.

Current capabilities within the Coast Guard to specifically address drones over critical infrastructure is limited by authority that is authorized by the Secretary to be able to take specific action, and that’s not organic capability that is at the local sector level. Our maritime security forces have a counter-UAS capability, but that requires specific authorization.

So our ability to counter——

Mr. HIGGINS. Do you have—let me just interject, Admiral.

Do you have the authority at the field level to make aggressive law enforcement decisions like seizing technology like to which I just described?
Admiral Arguin. Congressman, we have the ability to engage our partners to be able to investigate when those anomalous activities are happening, but as far as physical capabilities at the organic level, at the sector, those capabilities do not exist.

Mr. Higgins. I believe that should be our task, to address that as Congress, to make sure you have the necessary authority and that the laws are written to allow you to exercise that authority, and you have the technology required to protect our ports.

My time has expired, Mr. Chairman. I yield.

Mr. Gimenez. The gentleman yields.

I recognize the gentleman from New Jersey, Mr. Payne.

Mr. Payne. Thank you, Mr. Chairman.

The Transportation Worker Identification Credential, the TWIC program, helps protect secure areas of the ports by ensuring only individuals who have undergone TSA security threat assessments are provided access. However, TWIC vetting can serve as a barrier to employment, as individuals must visit an enrollment center to apply in person and then wait for TSA to conduct the vetting and ship a card back to them.

Applicants with a criminal history face additional delays, as TSA must manually adjudicate their eligibility. With more than 2 million individuals holding active TWIC cards, a significant portion of the U.S. workforce is reliant on the TWIC program for their livelihoods.

So I'm a strong believer in making sure that we provide avenues for formerly incarcerated individuals to re-enter the workforce or else they'll go back to whatever sent them away in the first place.

What does TSA do to minimize waiting times and reduce barriers for individuals with a criminal record who have served their time and are now—and are not disqualified by statute from holding a TWIC card?

Mr. Lattea. Thank you for that question.

This is an area that we do take a big focus on. We actually work with probation and parole boards to work with them on the redress process that was required underneath MTSA. This allows individuals to file waivers that we work through on that. The vast majority of people that file the waivers will receive the waiver.

It is a process they have to go through, and we help them through this often through second-chance events through probation, parole boards, and work very closely with them, too. So we have had great success on that in getting people back into the workforce.

Mr. Payne. Well, that's good to hear because, you know, whenever the issue was, that they made a mistake, and if it's not a disqualifying matter, then, you know, we have to do everything we can to reincorporate individuals into society or else, you know, God forbid, they'll return to, you know, bad habits.

So that's the major problem with folks out here. They come out; they're ready, but then, you know, there's no availability. Nobody wants to hire them. They said: You've done your time and you served your—and then—you know, you've done your time, you've served your purpose, but we're not going to hire you.

So and I appreciate that.
Rear Admiral, cyber threats continue to evolve and pose significant risks to critical infrastructure, including ports and maritime transportation systems. We have seen how destructive cyber attacks can be, as any attack that disrupts port operations can have a catastrophic, a cascading effect across U.S. economy.

Rear Admiral and Mr. Goldstein, do you believe that the Federal Government is providing port owners and operators with the resources and guidance and access to technical expertise they need to enhance their cyber defenses to the extent necessary to counter evolving threats?

Mr. GOLDSTEIN. Thank you, sir. It’s a really important question. From the point of view at CISA, we partner closely with Coast Guard both to make sure that we are staying on top of the cyber threat environment as it evolves and to urgently provide port owners and operators the timely information that they need to update their defenses. That could be in the form of published advisories that we often seal jointly between CISA and the Coast Guard to show that unity of message, or it could be technical information that we can share via more automated means.

We also work closely with the Coast Guard’s protection teams to make sure that they can benefit from the breadth of cross-sector information that CISA brings to bear. So, of course, given the pace of the evolving threat environment, we always have to keep moving faster than the adversary, but we are working urgently to make sure the port owners and operators have the information that they need to safeguard their systems against threats as they evolve.

Mr. PAYNE. Rear Admiral.

Admiral ARGUIN. Congressman, just to focus on the resources aspect of that, Coast Guard is heavily involved with FEMA’s Port Security Grant Program, and over the years, that grant program has provided funding and support for a variety of different protocols and items that can enhance security. Of late, there has been an emphasis on funding and supporting cyber protective grants.

Mr. GIMENEZ. The gentleman’s time has expired.

I now recognize the gentleman from New York, Mr. LaLota.

Mr. LALOTA. Thank you, Chairman.

Gentlemen, thanks for being here with us. Like a few of my colleagues, I want to focus most of my time on cybersecurity.

I represent New York’s First Congressional District, the east end of Long Island in Suffolk County, and Suffolk County is home to about 1.5 million people, and our county government has a budget of about $4 billion.

Last year, the Suffolk County government fell victim to a massive cyber attack and the impacts were devastating. Over a half a million people’s information was compromised. Hackers gained access to 470,000 driver’s licenses, 26,000 social security numbers, and 71 county systems. This attack time-warped the entire county back into the 1990’s, using pen and paper to take down 9–1–1 calls, taking away our access to geolocation devices, and forcing law enforcement officers to rely on finicky radios to respond to emergency needs.

While investigators into the cyber attack are still on-going, it’s clear there was a major cybersecurity failure and that we collec-
tively must do more as State, local, and Federal Governments to
do more for our folks.

Just about 50 miles away from my district is the Port of New
York and New Jersey, the largest container port on the East Coast.
In 2022 alone, the Port of New York and New Jersey moved ap-
proximately $271 billion worth of goods. As a security officer of the
Port of New York and New Jersey Greg Ehrle said, this port is the
gateway to one of the most concentrated consumer markets in
North America and most recently achieved status as the busiest
port in the United States.

We can only imagine what would happen if there was a cyber at-
tack on that port and what—to the like of what Suffolk County en-
dured. The impacts, I'm afraid, could be catastrophic, which leads
me to my first question to the admiral, sir. Can you discuss with
the committee the role of the Coast Guard's cyber protection teams
in helping ports mitigate cyber vulnerability, sir?

Admiral ARGUIN. Congressman, the Coast Guard's cyber protec-
tion teams are a team of 39 individuals that are highly-trained
technical specialists that are able to evaluate, assess networks, to
look for anomalies on those networks, and then provide feedback
to those network owners on ways that they can shore up potential
vulnerabilities.

They are directly connected with CISA's teams as well so that we
all share information to identify emerging threats and vulnerabilities and to be able to provide advice back to those enti-
ties to find ways to close those vulnerabilities.

If there is an attack, then that team can also come in and pro-
vide cyber forensics support in support of CISA, as well as Federal
law enforcement to not only restore network capability or give the
all-clear that that network can resume normal operation when it's
safe to do so, but that unique skill set is able to be provided to
those port stakeholders from an assessment perspective but then
also from a response perspective to resume normal operations as
soon as possible.

Mr. LAIOTA. Admiral, given that we all probably agree that the
threat is growing and its impact could be devastating, do you feel
like we're on the right trajectory with respect to where our leader-
ship is going and where our resources are being allotted in this
field?

Admiral ARGUIN. Congressman, I can certainly speak to the com-
mandant's perspective on the growing challenges that cyber poses
across the entirety of the marine transportation system and our in-
vestments in expanding. We've got a third cyber protection team is
being established on the West Coast, and that demand signal con-
tinues to grow to provide the right skill sets to support the Nation's
ports.

Mr. LAIOTA. Thanks, Admiral.

Mr. Goldstein, following the Colonial Pipeline ransomware attack
in 2021, TSA issued several cybersecurity regulations requiring
pipeline owners and operators to improve their cybersecurity prac-
tices. They've also extended the cybersecurity regulations to the
rail and aviation sectors.

My question is, sir: Looking at the devastating impact of the Co-
lonial ransomware attack, has CISA or Coast Guard considered ad-
ditional cybersecurity regulations for our maritime ports? If so, how are you working with affected stakeholders to develop these regulations?

Mr. Goldstein. I'll defer to my colleagues at Coast Guard and TSA on any plans they may have for future or current regulations.

I will say, at CISA, our goal is to really establish that baseline of technical measures that are most effective against the threats that we are seeing. Last fall, and then refreshed this spring, we released our cybersecurity performance goals, as directed via a Presidential national security memorandum, and these performance goals are really that succinct set of the most effective security practices prioritized by complexity, cost, and impact that all entities can use on a voluntary basis to know where to invest next and our partners with compulsory authorities can look to as a common resource across sectors.

Mr. LaLota. Thank you.

My time has expired. I yield, Mr. Chairman.

Mr. Garcia. Thank you, Mr. Chairman.

I want to thank all of our witnesses. Thank you for your service.

I'm proud to represent Long Beach and the Port of Long Beach, and Port of Long Beach and LA, of course, are the largest port complex in the United States as it relates to cargo container volume. I was mayor there for 8 years. The port there is a department of the city, and so I'm very involved in, obviously, port security and many of the issues that are being discussed today.

I'm also proud to co-chair the Congressional Ports Caucus and understand how critical port infrastructure is to the Nation's economy.

I want to talk about the security piece just a little bit as well. I know that ports being not just an economic driver but also critical in security and critical in something that we're all interested in, I wanted to mention some of the—you know, some of the comments that were being made today, which I think a little bit, some of them, are a little off the mark.

I'm not sure if anyone here knows how many automated ports there are in the United States. Anyone have an idea?

There's actually only 4 ports, terminals that are actually automated of the 360 terminals that we have in the United States, and I mention that because there have been comments also in reports and in the media about access and the ability for maybe foreign actors to interfere with some of these automated cranes and automated terminals.

Why don't I just give you an example. For example, in my district, of course, thanks to the ILWU and so many other workers, every single crane can be operated manually. We have one automated terminal there that can also be switched in an emergency to completely be operated manually.

There have been folks that have, in the Majority, that have claimed, and I'll quote: “If an adversary exploits the operational technology system of these cranes, our port operations could be completely shut down.”
You know, not just me but the American Association of Ports called that alarmist and sensationalized. While we should take port security as a critical issue we should discuss and seriously, it’s important to remember that there is no foreign power that can somehow infiltrate our terminals and shut down our ports as it relates to automated cranes.

Mr. Goldstein, now, we do know that hackers have actually shut down terminals in a different way before. Is that correct?

Mr. GOLDSTEIN. I’m sorry, sir. Would you repeat the——

Mr. GARCIA. We know that hackers have shut down ports before in different ways but not through cranes. Is that correct?

Mr. GOLDSTEIN. Sir, I don’t have off the top of my head a specific example where a hacker has shut down a port terminal.

Mr. GARCIA. I’ll mention that we had in San Diego, actually, a cyber attack that took down a cargo carrier. It was a Maersk cargo container, a carrier. The computer network got shut down. It caused great damage. So these are the issues around cybersecurity that are really critical, I think, as it relates to ports.

But we also should talk about, when we have these discussions, more system-wide vulnerabilities. Do you think the Port Security Grant Program, which funds cybersecurity organizations, is an important tool to make sure that our ports are actually safe from espionage or hacking?

Mr. GOLDSTEIN. Yes, sir. Absolutely.

Mr. GARCIA. Well, thank you.

I also agree that the Port Security Grant Program is critical for ports across the country, and I mention that because every single Republican Member of this committee actually voted to slash that program, along with other grant programs as well.

Now, I take competition with China and port security also very seriously, but this discussion is not exactly directed at that.

I want to thank you all for your commitment to investing in the country, investing in overall broad port security, and your support for the Port Security Grant Program.

I yield back.

Ms. LEE [presiding]. Thank you, Mr. Garcia.

At this time, I believe I will recognize myself for the purpose of 5 minutes of questioning.

I am proud to represent a portion of the city of Tampa, and ensuring proper security at the Port of Tampa is a key priority for Florida and for our Nation. Our port helps move 33 million tons of cargo per year and is responsible for $17 billion of economic impact.

When it has—it is a major cruise home port and also a shipyard repair center. When it isn’t operating, as is the case during occasional natural disasters, the entire region experiences shortage of fuel, food, and other essentials.

I’d like to focus my questions on you, Assistant Director Goldstein, to start out. One thing that you mentioned during your opening statement was the Maritime Sector Government Coordinating Council. Would you please elaborate on the GCC, the purpose of it and what it does?

Mr. GOLDSTEIN. Yes, ma’am. Absolutely.

One of the most valuable authorities that Congress has vested in CISA is the Critical Infrastructure Partnership Advisory Council
Authority called CIPAC. That allows us to bring together partners from the private sector with relevant Government agencies in a trusted forum where they can be candid and transparent about the risks that they are seeing and work with partners both in industry and Government to identify shared and common solutions.

So we do this work with multiple sectors. In this case, with our partners at Coast Guard, we bring together partners in the maritime sector to have just these candid conversations about the risks that our partners are seeing so that we can develop shared solutions together on an on-going, sustained basis.

Ms. Lee. You mentioned in your testimony that one of the things you were working on in the GCC was developing sector-specific goals in the maritime sector. What is your timeline and your process for actually developing those sector-specific goals that we can then be using as a metric for measuring our success?

Mr. Goldstein. Yes, ma’am.

Our goal with developing sector-specific cybersecurity performance goals is to really, in the first instance, be led by our industry partners and the sector risk management agency; in this case, our partners at Coast Guard. So we are working now with Coast Guard and maritime stakeholders to understand the gaps that sector-specific goals could help fill that would be additive to the cross-sector goals that we’ve already developed.

But the real key point here is, because these goals are voluntary, they need to add value, and so we want to make sure that our maritime sector stakeholders, as with stakeholders across critical sectors, see voluntary value in these goals. We’re ideally going to be led by their efforts instead of imposing an artificial timeline that may yield an end result that actually isn’t useful to help our partners reduce their risks.

Ms. Lee. Tell us, if you would, more about the cyber storm training exercise and the private-public partnership that is part of that exercise.

Mr. Goldstein. Yes, ma’am. Absolutely.

One of the most important things that we can do as a national, indeed, even global security community is come together to test our processes, test our activities against real-world scenarios and make sure that they are actually fit for purpose. So the cyber storm exercise is conducted recurrently with different scenarios each time, bringing together not just partners in government but also partners in the private sector, particularly partners like the Information Sharing and Analysis Centers, or ISACs, that cover, of course, countless organizations across sectors to make sure that, when an incident does happen, we know how we’re going to share information, what we’re going to share, and, most importantly, that we have these processes and relationships well-established and codified so we’re not doing this work for the first time when an incident occurs.

Ms. Lee. What is CISA’s role in the ISACs?

Mr. Goldstein. So CISA’s role in the ISACs is largely to be a cross-sector provider of timely and actionable information. So, for example, through our Joint Cyber Defense Collaborative, we continuously derive actionable information from industry partners, from the intelligence community, from international cyber defense
agencies, and from our own sensors deployed across Government networks. We then bring that information in. We enrich it with insights from Government and from industry partners with unique visibility, and then we share it out broadly.

The ISACs provide that mechanism so that a piece of information can be shared not just with a few entities but with thousands instantaneously. They provide that mechanism to provide both those cross-sector insights but also go deep into a sector when the information so dictates.

Ms. Lee. How are you utilizing the partnership and the information you receive from your private-sector partners to help build those sector-specific goals and strengthen the infrastructure overall?

Mr. Goldstein. Yes. That’s a good question, ma’am.

One of the biggest challenges in cybersecurity today is to understand the unique vulnerabilities that are facing particular sectors and the unique ways that adversaries are targeting each particular sector. So information from our partners in industry that is specific to incidents, intrusions, campaigns targeting a different sector will help us make recommendations to the specific controls or risk-reduction measures that can help the sector maximize its security which we can then codify in the performance goals.

Ms. Lee. All right. Thank you, sir.

I do believe that my time has now expired.

I now recognize the Ranking Member.

Mr. Thanedar. Madam Chairlady, thank you so much. I love Tampa. I love your home town.

Thank you all for being here and thank you for your testimony.

I want to go back. I know the Rear Admiral didn’t get a chance to answer my last question. I want to go back to the TWIC card. Mr. Latta said, what, about 60 percent of them get their cards in, what, 6 to 10 days?

Mr. Latta. Seven to 10 days.

Mr. Thanedar. Seven to 10 days. But we can do better because people rely on these cards for their livelihood, the truck drivers, the port workers.

So my question really is, how can we expedite these processes in terms of implementation of the requirements of the Safe Port Act of 2006? I know the Coast Guard has delayed implementation of the electronic TWIC and biometric readers. How can we use technology to speed up this process so people can have these cards faster and be able to work?

Admiral Arquin. Ranking Member, so the TWIC reader rule implementation, we’re currently evaluating the Rand Corporation’s study on where we should have those TWIC readers to better inform and manage the risks that are associated with the facility and vessel security. So once—we’ve also pushed that report to our National Maritime Security Advisory Committee, Federal advisory committee, that will help inform ideas and recommendations on where we should take a reasonable approach to evaluating risks within the port to make sure that access control, whether it’s secured or restricted access, is appropriate for the risks that are out there within our ports.

Mr. Thanedar. OK. Thank you.
Mr. Latta, as TSA contracts with additional providers for PreCheck enrollments, how will you assess the continued health of the Universal Enrollment Service Program, which covers PreCheck, TWIC, and Hazmat enrollments, to ensure the continued ability of my constituents and workers across the country to apply for and receive their TWIC cards?

Mr. Latta. Yes. Thank you for that question.

So we are Congressionally-mandated to do expansion on TSA PreCheck for enrollment providers. We’re in the process of bringing two additional providers on. We do think that—we do not think that that will have an effect on the UES provider. There’s still 570 enrollment centers that are open, many are in every State, in every territory, and around critical infrastructure locations that need those.

So we do think that that will still remain, and there’s a contractual obligation on that too to have those sites up and running during that time.

Mr. Thanedar. Thank you, Mr. Latta.

Madam Chair, I yield back.

Ms. Lee. The gentleman yields back.

I now recognize the gentleman from Louisiana for an additional question.

Mr. Higgins. Thank you for the time for an additional question, Madam Chair.

Mr. Goldstein, to clarify for America, CISA has authority over—regarding cybersecurity in our ports. Correct?

Mr. Goldstein. Sir, CISA has broad authority——

Mr. Higgins. OK.

Mr. Goldstein [continuing]. To provide cybersecurity assistance to cross-sectors, yes.

Mr. Higgins. That’s where I’m going.

So the Port of Lake Charles, for instance, in my district is a hub of energy export sector of the entire country, including LNG and petrochemical products. The coordinated effort between many private entities sort-of intersect there in the port environment. You could have scores of business entities that are involved in that operation that intersect right there, pipelines, utilities, transport, the port itself, chemicals. There’s many, many layers of operators there. Any one of them could have some random employee that works in their IT department detect a threat in the dead of night. They don’t stop working. They work 24/7, 365.

So are you accessible? What is the communications system at 2 o’clock in the morning on a holiday weekend, a Saturday night? If I’m an IT worker at a pipeline and I detect a cyber threat——

Mr. Goldstein. Yes.

Mr. Higgins [continuing]. How do I reach you?

Mr. Goldstein. Yes, sir, absolutely. Let me give two answers.

The first to your question, sir, is we have a 24 by 7 watch floor. It is called CISA Central. It is manned around the clock, and so organizations across the country can report a cyber incident and get a response at any time.

I will also add, sir, we have regional cybersecurity experts, including in and around your district, whose role it is to build these deep relationships with operators of critical infrastructure of cross-
sectors so that not only can we help to build resilience before an incident occurs, but when something happens, they have somebody in the area who they know and trust.

Mr. Higgins. Is that by telephone or by email?

Mr. Goldstein. So, sir, for CISA Central, it can be reached by phone, by email, or by an on-line report.

Mr. Higgins. So, if I'm an IT employee at a pipeline and I feel strongly enough about a threat, I'd be able to talk to a human being at CISA on a telephone in the dead of night on a weekend—

Mr. Goldstein. Yes, sir.

Mr. Higgins [continuing]. To help walk me through what the next step is on responding to this threat?

Mr. Goldstein. Yes, sir.

Mr. Higgins. That's reassuring.

Thank you for that answer.

Madam Chair, I appreciate the additional time, and I yield.

Ms. Lee. The gentleman yields back.

I 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 witnesses, 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, the subcommittee stands adjourned.

[Whereupon, at 3:08 p.m., the subcommittee was adjourned.]
QUESTIONS FROM HONORABLE ROBERT GARCIA FOR WAYNE R. ARGUIN, JR.

Question 1. How have USCG and CISA provided direction to public and private-sector organizations who aim to leverage USCG’s Maritime Cybersecurity Assessment and Annex Guide and CISA’s Marine Transportation System Resilience Assessment Guide?
Answer. Response was not received at the time of publication.

Question 2. I would like to address how USCG, CISA, and TSA are aligning together to address port security risks, especially cyber risks. In January 2023, USCG released the Maritime Cybersecurity Assessment and Annex Guide, while in March CISA released the Marine Transportation System Resilience Assessment Guide in collaboration with the U.S. Army Corps of Engineers (USACE).
Based on feedback I received from stakeholders, CISA and USCG personnel who coordinate with the maritime sector were unaware of their counterpart agency’s strategy.
To what extent did USCG and CISA collaborate with each other in developing these Guides?
Answer. Response was not received at the time of publication.

Question 3. With the release of the administration’s National Cybersecurity Strategy in March, what efforts have been made or are planned to ensure that USCG, CISA, and TSA are working together to synchronize their efforts to safeguard our Nation’s ports?
Answer. Response was not received at the time of publication.

Question 4a. Ports serve as the intermodal hubs for maritime, rail, pipelines, and highways to connect supply chains. What alignment is happening between USCG, CISA, and TSA to provide critical infrastructure stakeholders with timely threat information and create a single mechanism for incident reporting to Federal agencies?
Answer. Response was not received at the time of publication.

Question 4b. How are your agencies scaling public-private collaboration with Information Sharing and Analysis Centers (ISACs)?
Answer. Response was not received at the time of publication.

Question 4c. Are there cybersecurity regulations being developed as outlined in the National Cybersecurity Strategy to address risks associated with ports? If so, are those regulations being developed in collaboration with critical infrastructure owners and operators?
Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN CARLOS A. GIMENEZ FOR ERIC GOLDSTEIN

Question 1. How have USCG and CISA provided direction to public and private-sector organizations who aim to leverage USCG’s Maritime Cybersecurity Assessment and Annex Guide and CISA’s Marine Transportation System Resilience Assessment Guide?
Answer. Response was not received at the time of publication.

Question 2. I would like to address how USCG, CISA, and TSA are aligning together to address port security risks, especially cyber risks. In January 2023, USCG released the Maritime Cybersecurity Assessment and Annex Guide, while in March CISA released the Marine Transportation System Resilience Assessment Guide in collaboration with the U.S. Army Corps of Engineers (USACE). Based on feedback I received from stakeholders, CISA and USCG personnel who coordinate with the maritime sector were unaware of their counterpart agency’s strategy.
To what extent did USCG and CISA collaborate with each other in developing these Guides?
Answer. Response was not received at the time of publication.

**Question 3.** With the release of the administration’s National Cybersecurity Strategy in March, what efforts have been made or are planned to ensure that USCG, CISA, and TSA are working together to synchronize their efforts to safeguard our Nation’s ports?

Answer. Response was not received at the time of publication.

**Question 4a.** Ports serve as the intermodal hubs for maritime, rail, pipelines, and highways to connect supply chains. What alignment is happening between USCG, CISA, and TSA to provide critical infrastructure stakeholders with timely threat information and create a single mechanism for incident reporting to Federal agencies?

Answer. Response was not received at the time of publication.

**Question 4b.** How are your agencies scaling public-private collaboration with Information Sharing and Analysis Centers (ISACs)?

Answer. Response was not received at the time of publication.

**Question 4c.** Are there cybersecurity regulations being developed as outlined in the National Cybersecurity Strategy to address risks associated with ports? If so, are those regulations being developed in collaboration with critical infrastructure owners and operators?

Answer. Response was not received at the time of publication.