CSC 2.0

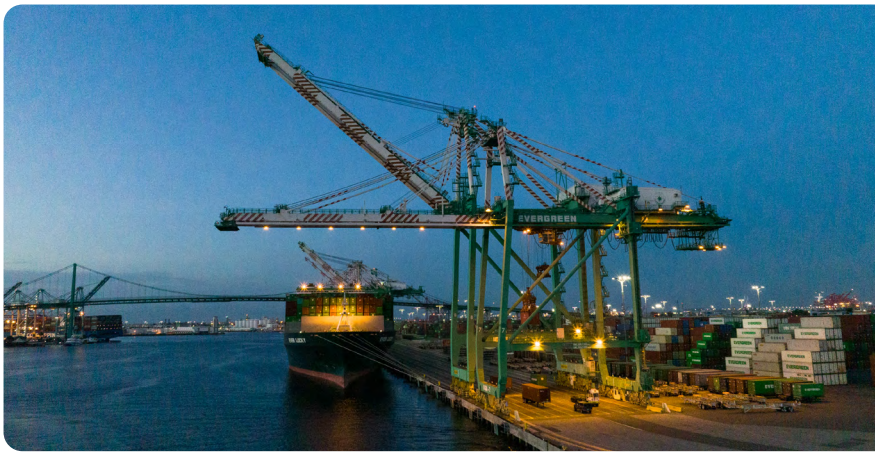
March 2023

Full Steam Ahead: Enhancing Maritime Cybersecurity

Jiwon Ma
William Loomis

Table of Contents

Executive Summary



U.S. waterways provide energy-efficient transportation options to move goods and people, but hackers have increasingly targeted the maritime industry.

Since its inception, the United States has been a maritime nation dependent on its maritime transportation system (MTS) as vessels evolved from manpower-intensive wooden sailing ships to highly automated container ships. The U.S. MTS consists of approximately 25,000 miles of navigable waterways, 250 locks, 3,500 marine terminals, 29 container ports, thousands of recreational marinas, as well as the Great Lakes and St. Lawrence Seaway.[1] This infrastructure supports the tens of thousands of container ships, oil and gas carriers, chemical tankers, tugs and barges, cruise ships, ferries, and other vessels that drive a large portion of the U.S. economy and global trade.

In this vital subsector of U.S. transportation, operators rely on technologies and industrial control systems to navigate, communicate, and control various aspects of maritime operations vital to national security and prosperity. It is a highly distributed, diverse subsector composed of subsystems — ships, ports, shipping lines, shipbuilders, cargo handlers, traffic controllers, and many more — each of which represents a network of systems on its own.

A cyberattack against a complex maritime ecosystem could be devastating to the stability of the global economy. U.S. government and industry efforts to protect against such attacks, however, are lagging.[2]

In its March 2020 final report, the congressionally mandated Cyberspace Solarium Commission repeatedly highlighted the need for better government-industry cybersecurity collaboration and better resourcing of government efforts to support the private sector. Picking up on this theme, a group of scholars at the Atlantic Council (including one of this report's co-authors) published *Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity*,[3] which proposed short- and long-term solutions to improve the cybersecurity of the MTS. Building on that monograph's foundation, this report provides additional analysis of cyberattacks against the MTS along with recommendations to resource the subsector's cybersecurity more fully.

The report is divided into three sections. The first section looks at how the cyber threat to the MTS has evolved in recent years. The next discusses U.S. government efforts to address cyber issues affecting the MTS. Last is a section with recommendations for Congress to ensure uninterrupted commerce and the movement of goods and people across U.S. borders.[4]

If Congress acts on these recommendations, it can empower the MTS subsector by providing additional resources and grant-funding opportunities; supporting agencies in testing the resilience of the subsector's operational technology (OT); and directing the U.S. Coast Guard (USCG) to develop programs to address challenges in the workforce. Lastly, in the tradition of the Cyberspace Solarium Commission, this report offers sample legislative text to demonstrate how lawmakers could implement these recommendations.

Acronyms

Captain of the Port	COTP
Cyber Testing for Resilient Industrial Control Systems program	CyTRICS
Cybersecurity and Infrastructure Security Agency	CISA
Department of Homeland Security	DHS
Department of Transportation	DOT
Government Accountability Office	GAO
Maritime Transportation Security Act of 2002	MTSA
maritime transportation system	MTS
MTS-Information Sharing and Analysis Center	MTS-ISAC
National Defense Authorization Act	NDAA
operational technology	OT
Port Infrastructure Development Program	PIDP
Presidential Policy Directive 21	PPD-21
Sector Risk Management Agency	SRMA
Transportation Security Administration	TSA
U.S. Coast Guard	USCG
U.S. Committee on the Marine Transportation System	CMTS
United States Transportation Command	TRANSCOM

A Vital Subsector of U.S. Critical Infrastructure Under Threat

Since at least 2017, hackers have increasingly targeted the maritime industry, disrupting key port operations and causing significant financial damage to affected companies and the global economy.

The MTS is an essential component of the U.S. economy — especially international trade — and contributes to national security. More than 75 percent of the nation's trade relies on various interdependent elements of the MTS, which accounts for $5.4 trillion in economic activity[5] and $1.5 trillion in imports[6] while providing more than 30 million jobs. In 2020, $259 billion in trade passed through the Port of Los Angeles alone.[7]

U.S. waterways provide energy-efficient transportation options to move goods and people. At marine terminals, ships and vessels load and unload people and cargo from waterborne transportation to ports connecting the highways, railways, pipelines, and airports that make up the rest of the transportation sector. As of October 2021, according to *Raising the Colors*, the MTS "feeds a quarter of US gross domestic product."[8] The report noted that prior to the Covid-19 pandemic, "commercial shipping moved close to 80 percent of global trade by volume and over 70 percent of global trade by value."[9] A more recent estimate by the USCG put the figure for global trade by volume at 90 percent.[10]

The energy sector, in particular, is closely tied to the MTS. U.S. gas exports flow through a small number of specialized ports for liquefied natural gas (LNG) and travel to Europe and elsewhere on LNG-specific maritime craft. With improvements to LNG export facilities, the United States is expected to become the world's largest exporter of LNG by the end of 2023.[11] This growth is crucial to stabilizing global energy prices and supporting European allies as they seek independence from Russian energy exports. However, the importance of LNG exports also increases the risk of cyberattacks on the MTS by Russian state-backed actors, cyber criminals, and hacktivists.

Finally, commercial shipping is vital to U.S. military capabilities. United States Transportation Command (TRANSCOM) notes that in the fiscal year 2020, commercial sea freight shipping providers accounted for 55 percent of cargo transported for contingency operations and for 95 percent of steady-state operations — reflecting $877 million in TRANSCOM's contracting portfolio of sealift services.[12]

Cyber threats against the MTS have intensified alongside the growing interconnectedness of the industry to the global economy, security, and trade. In June 2017, Russia's NotPetya malware attack on Ukraine spread around the world, infecting global shipping giant Maersk, which is responsible for 76 ports globally and hundreds of vessels carrying tens of millions of tons of cargo at any moment. Port operations halted, container ships could not unload, and trucks could not enter ports to move cargo. Weeks later, after hundreds of millions of dollars in damages, operations returned to normal.[13] While no single cyber incident since 2017 has dramatically affected global shipping, the MTS has remained under constant attack.

In November 2019, a UK-based maritime engineering services provider, James Fisher and Sons PLC, suffered a cyberattack in which malicious actors accessed the company's network, restricting access to financial and communications systems.[14] In April 2020, a malware attack damaged computer systems at the Mediterranean Shipping Company's headquarters in Geneva, causing data center outages that crashed the company's website and consumer portal.[15]

In a bright spot, in August 2021, the Port of Houston quickly discovered a breach in its systems and followed its Facility Security Plan, preventing the attackers from disrupting operational systems or corrupting or stealing data. The U.S. Coast Guard Cyber Command analyzed the incident, and Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS), testified before Congress that a nation-state actor was likely responsible.[16]

More recent incidents have not had such positive outcomes. In early February 2022, a ransomware attack hit oil storage and loading facilities at the Amsterdam-Rotterdam-Antwerp port, disrupting operations. Days earlier, Oiltanking GmbH and Mabanaft GmbH, two subsidiaries of German logistics firm Marquard & Bahls, suffered a ransomware attack, disrupting energy terminals in Germany.[17] Together, the two apparently unrelated incidents caused delays in the movement of energy products, including heating oil, diesel, jet fuel, gasoline, and fuel oil in Europe.[18]

On December 25, 2022, the Port of Lisbon announced it had suffered a ransomware attack affecting its website but reassured the public that the attack did not compromise operational activities.[19] Ransomware group LockBit threatened to leak stolen confidential data if the port refused to pay a $1.5 million ransom.[20] Two weeks later, on January 7, 2023, an Oslo-based ship classification society, DNV, suffered a ransomware cyberattack, affecting approximately 15 percent of its vessels in operation,[21] or 1,000 vessels and 70 customers.[22] The hackers targeted DNV's maritime fleet management software, forcing it to shut down servers.[23]

To date, the damage from cyberattacks against ports and shipping companies has been localized and contained. While the attacks are significant, none has had cascading effects across other sectors of the global economy. Had any of the victims been less resilient or less able to pay a ransom, the effects of the attacks would likely have been more severe.

Efforts to Improve Cyber Resilience

Interagency efforts have evolved over several decades to address not only the physical security of the MTS but also the growing cybersecurity challenges. This section reviews the Maritime Transportation Security Act of 2002, how it evolved to address cybersecurity challenges, the role of the USCG in protecting the MTS, and ongoing interagency policy efforts to build the cyber resilience of the MTS.

In February 2013, Presidential Policy Directive 21 (PPD-21) designated the transportation sector and 15 other sectors of the economy as critical infrastructure, assigning each a federal sector-specific agency, later named a "Sector Risk Management Agency," or SRMA.[24] Under federal law, SRMAs are responsible for supporting sector risk management, assessing sector risk, leading sector coordination, facilitating information and intelligence sharing, supporting incident management, and contributing to emergency preparedness efforts.[25]

The transportation sector has co-SRMAs, DHS and the Department of Transportation (DOT). DHS has delegated its SRMA duties for the MTS to the USCG.[26] The Coast Guard and Maritime Transportation Act of 2012, meanwhile, established the U.S. Committee on the Marine Transportation System within DOT to serve as the federal interagency coordinating committee.[27]

Long before PPD-21, in the wake of the September 11 attacks, policymakers recognized how vital it is to secure U.S. ports and maritime transport. The Maritime Transportation Security Act of 2002 (MTSA), a landmark legislation signed by President George W. Bush, required port authorities and vessel operators to enact security measures to protect against terrorist attacks.[28] The law originally focused on identifying and mitigating physical threats but was subsequently amended to include cybersecurity requirements.[29] Facilities regulated by the MTSA are now required to complete cyber risk assessments and incorporate cybersecurity into their Facility Security Assessment and Facility Security Plan.[30]

To assist MTS stakeholders in addressing cyber risks as part of their Facility Security Plan, the USCG published its latest Maritime Cybersecurity Assessment and Annex Guide in January 2023, a more comprehensive version of its earlier guide from March 2020.[31] These non-binding guides serve as resources for those implementing cyber risk assessments as required for MTSA-regulated facilities. The March 2020 version is useful for meeting baseline standards of conducting cybersecurity risk assessments. However, the new version provides additional guidance that could be useful not only for assessing the cybersecurity risks of MTSA-regulated facilities but also for continuing to monitor improvements in existing security measures at U.S. ports.

In December 2020, the Trump administration, in an attempt to strengthen MTS cyber resilience, issued the National Maritime Cybersecurity Plan,[32] which provides a roadmap for U.S. government departments and agencies to work with the private sector to manage and reduce cyber risk. The plan, however, was more of a strategic guide and less geared toward implementation. Progress on the plan has been limited since the previous administration issued it in the last month of its tenure to departments and agencies that are often slow to act on cybersecurity.

The Biden administration, for its part, has attempted to improve the cyber resilience of all critical infrastructure and specifically the MTS. In August 2021, the USCG issued an updated Cyber Strategic Outlook,[33] which centers on three lines of effort: to defend and operate USCG networks, identify and manage cyber risks to the MTS, and "fight and win" in cyberspace.[34] The strategy details the USCG's roles and responsibilities as an SRMA in protecting MTS from cyber risks. In the previous version of the strategy, released in 2015, the USCG committed to developing global maritime cyber prevention and response protocols.[35] The 2021 strategy is a culmination of the USCG's efforts to develop the prevention and response framework. It emphasizes the USCG's commitment to carry out its SRMA responsibilities, which includes supporting incident management.[36]

The 2021 strategy also highlights the valuable role played by the captain of the port (COTP). Designated by the Coast Guard commandant, the COTP serves as a port's federal maritime security coordinator and ensures its safety. COTPs also execute prevention and response frameworks for critical incidents and mission needs.

A unique feature of the USCG's capabilities and relationship with the MTS is its cyber advisors, USCG civilian employees who advise the COTPs by providing contextual information on cyber-related matters. Cyber advisors play a vital role in conducting risk assessments of the MTS subsector. In the "United States Coast Guard Strategy," published in October 2022,[37] the USCG committed to executing the Ready Workforce 2030 Strategic Outlook, which emphasizes the need to offer "non-monetary, incentives-based reenlistment alternatives" to compete with the private sector.[38] These latest updates signal a positive step toward better securing the MTS. However, there is a pressing need for the USCG to continue maturing and expanding its programs.

The USCG faces challenges in identifying appropriate civilian cybersecurity talent, partly because it lacks information on the diverse skill sets required to support its mission needs. According to a recent report by the Government Accountability Office (GAO), the USCG is not yet using a standard to assess its cyber workload or workforce.[39] For instance, the USCG lacks information on 55 percent of its authorized and funded cyber workforce positions in three headquarters units.[40] DHS officials agree with GAO's assessment, and the USCG's Office of Cyberspace Forces will release a workforce management plan addressing these issues by September 29, 2023.[41]

The USCG is also making ongoing efforts to build external cybersecurity partnerships, especially with CISA. CISA and the USCG coordinate the release of alerts and advisories for the MTS. For instance, CISA and USCG Cyber Command released a

joint advisory in June 2022 detailing the continued exploitation of the Log4Shell vulnerability by malicious cyber actors.[42] CISA and USCG utilized USCG intelligence operations and collaborated with private sector partners in the MTS and technology industries to provide specific information and technical analysis detailing indicators of compromises in two incidents.[43]

This partnership is valuable, as are joint CISA-USCG efforts to streamline reporting and coordination. Given the range of government stakeholders in the subsector, however, collaboration would be more effective if it incorporated the Transportation Security Administration (TSA), which serves as the SRMA for other transportation subsectors; Customs and Border Protection; the Federal Bureau of Investigation; and TRANSCOM.

Industry, meanwhile, has its own set of collaboration mechanisms. In particular, the MTS-Information Sharing and Analysis Center (MTS-ISAC) serves as a centralized point of coordination, collaboration, and information sharing.[44] The organization provides a forum for sharing timely and actionable cyber threat information across the MTS community worldwide and issues its own actionable advisories for members. MTS-ISAC encourages engagement with the USCG and other government partners, noting on its website that the information it provides can assist organizations in meeting cyber requirements under the MTSA.[45]

In October 2022, CISA issued its Cybersecurity Performance Goals for all critical infrastructure[46] as required by the July 2021 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems.[47] These are voluntary baseline measures that CISA urges all critical infrastructure owners and operators to adopt to improve their cybersecurity. As a next step, CISA is working with SRMAs, including the USCG, to develop sector-specific guidance. It is also working with government partners to harmonize cyber incident reporting requirements and structures for all critical infrastructure.[48]

Recommendations for Congress

While government and industry partners are committed to securing the MTS, the scope, scale, and severity of cyber threats are growing. More must be done to protect this system of systems that is vital to national security and economic prosperity. The Atlantic Council report outlines actions that the federal government, international organizations, and industry should take. These include near-term priorities like creating a global clearinghouse for MTS intelligence (which, to some extent, the MTS-ISAC is providing); mid-term priorities like better OT security for global maritime energy networks; and longer-term priorities like a push to make cybersecurity a core component of conventional maritime insurance. The 2020 National Maritime Cybersecurity Plan presents a similarly ambitious set of proposals to organize federal efforts to secure the supply chain; improve risk management and set standards; share information and intelligence; and bolster the maritime cybersecurity workforce.

Congress has an important role to play in providing resources and direction to improve the cyber resilience of the MTS. In concert with the Atlantic Council's recommendations, the following recommendations focus on addressing challenges with resource allocation and workforce development as well as highlighting a potentially valuable policy idea left on the cutting room floor during prior legislative cycles.

1. Mandate increased resources for the USCG to support its responsibilities as an SRMA.

The DHS should request, and Congress should mandate, increased funding for the USCG to support its SRMA responsibilities, including building out a cybersecurity program under the USCG's SRMA office. While only 2.8 percent of the USCG's operations and support budget funds cyber and intelligence operations,[49] in the fiscal year 2022, the USCG saw the largest funding reductions from previous years in areas supporting cyber missions.[50] Once funding is increased, the USCG should use the additional resources to enhance collaboration with organizations like the MTS-ISAC and to leverage MTS-ISAC's existing capabilities to ensure all industry stakeholders receive timely and actionable threat information and have the information they need to implement cybersecurity best practices and requirements.

2. Establish an OT test bed within CISA to identify potential cybersecurity vulnerabilities for critical systems used within the MTS.

CISA, in close partnership with the USCG and maritime private sector partners, should establish a maritime OT supply chain testing capability to test the cyber resilience of critical maritime OT, like the Department of Energy's Cyber Testing for Resilient Industrial Control Systems program (CyTRICS). CyTRICS utilizes the strategic partnerships, facilities, and analytical capabilities of six national laboratories to conduct tests of OT to improve design and manufacturing, provide a more in-depth understanding of the sector's threat environment, and create an operational pathway for meaningful public-private partnership.[51] Similarly, the USCG's collaboration with CISA's National Infrastructure Simulation and Analysis Center[52] could facilitate an OT test bed program to identify potential cybersecurity vulnerabilities in existing infrastructure. CISA would provide the USCG with a strategic partnership with national laboratories to conduct OT test bed programs for maritime components. The program can begin by testing for cybersecurity vulnerabilities in foreign-manufactured cranes used in U.S. ports — as mandated by the National Defense Authorization Act (NDAA) of the fiscal year 2023 — and then expand into broader, systemically important maritime OT.

3. Require USCG participation in grant programs that will ensure sufficient funding for mitigating MTS cyber risk.

DHS should ensure there is sufficient grant funding to mitigate cyber risk in the MTS by requiring USCG participation in the Port Infrastructure Development Program (PIDP) and the Port Security Grant Program. The bipartisan Infrastructure Investment and Jobs Act of 2021 will provide $450 million annually through 2026 to improve America's ports and waterways through the PIDP.[53] The PIPD provides competitive grants for port modernization and expansion to improve ports' resiliency, including technologies and cybersecurity supporting the OT of port systems. Furthermore, the fiscal year 2022 Appropriations Act allocated an additional $234.3 million for the PIDP, for a total of $684.3 million in funding for the fiscal year 2022, the highest level of investment since the program's inception.[54] Meanwhile, in August 2022, the DHS announced that its Port Security Grant Program would provide $100 million to protect and safeguard America's critical port infrastructure.[55] The program emphasizes improving cybersecurity[56] and identifies it as a priority area but does not set a minimum spending requirement.[57] Congress should take steps to ensure that a minimum of 8 percent of the Port Security Grant Program's funding goes toward investments in cyber risk mitigation and that a minimum of 5 percent of the PIDP's funding goes toward the same.[58]

4. Direct the USCG to develop cybersecurity education and workforce programs.

Congress should direct the USCG to develop a program to enhance MTS cybersecurity education and workforce programs, including a public-private workforce rotational program with portable credentialing. These programs can help build the needed pipeline of sector-specific cybersecurity expertise for both the civilian and military cybersecurity workforce. Effective cybersecurity education and workforce programs will provide training that delineates between mission operations and support functions. The programs should also make federal cybersecurity positions competitive with those of the private sector, if not directly through salary, then through professional development opportunities. These programs should be designed to increase sector and subsector cybersecurity training.

Conclusion

The maritime ecosystem and its supporting infrastructure are critical to U.S. national security, energy security, and economic stability. While government and industry partners have resources and knowledge, congressional action can expand pre-existing cybersecurity programs, foster new capabilities, and create a more secure ecosystem.

Appendix: Model Legislative Proposals

Sector Risk Management Agency Funding

This appropriations language implements the recommendation to fund the United States Coast Guard at a sufficient level to fulfill its sector risk management agency duties for the maritime transportation sector.

SECTOR RISK MANAGEMENT AGENCY DUTIES

For the necessary expenses of the Coast Guard for cyber and intelligence operations in support of its duty as the sector risk management agency for the maritime transportation sector; $5,000,000 to remain available until December 31, 2024.

Maritime Equipment Cybersecurity Test Bed

This proposal implements the recommendation to establish a Maritime Transportation System (MTS)-specific cybersecurity test bed within the Cybersecurity and Infrastructure Security Agency. The program would aim to identify high-priority operational technology (OT) components, perform expert testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing for maritime systems.

A BILL

To establish a program within the Cybersecurity and Infrastructure Security Agency to identify high-priority operational technology components, perform testing, share information about vulnerabilities in the digital supply chain, and inform improvements in component design and manufacturing for maritime systems.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. XXXX.

(a) Definitions.—In this section:

(1) Secretary.—The term "Secretary" means the Secretary of the Department of Homeland Security.

(2) Commandant.—The term "Commandant" means the Commandant of the United States Coast Guard.

(b) Establishment of the Maritime Ecosystem Cybersecurity Testing Center.—Not later than 18 months after the passage of this act, the Secretary, in consultation with the Commandant, shall establish a maritime transportation system-specific cybersecurity test bed within the Cybersecurity and Infrastructure Security Agency. The Center shall—

(1) conduct rigorous security testing to identify vulnerabilities in critical maritime operational technologies;

(2) develop new capabilities for vulnerability discovery, management, and mitigation within such technologies;

(3) audit software in critical maritime operational technologies or upon which critical maritime operational technologies are dependent;

(4) establish a vulnerability disclosure program and publish key vulnerabilities identified, with the goal of incentivizing participation from additional vendors; and

(5) serve as a primary technical training tool for both the Department of Homeland Security and United States Coast Guard Academy and United States Coast Guard personnel.

(c) Identification of Initial Devices for Testing.—Not later than 120 days after the establishment of the Testing Center under paragraph (b) the Secretary, in consultation with the maritime industry, the Commandant, the Director of the Cybersecurity and Infrastructure Security Agency, Federally funded research and development centers and national labs, and other agencies as determined by the Secretary, shall develop a comprehensive framework to identify critical maritime operational technologies.

(d) Annual Report to Congress.—The Secretary shall provide an annual report to the Senate Committee on Homeland Security and Governmental Affairs and the House Committee on Homeland Security, containing—

(1) a summary of the work performed by the test bed, including an explanation of how grant funding was allocated and a list of vulnerabilities found, along with the corresponding recommended mitigation process and an assessment of the criticality and severity of each vulnerability;

(2) a list of stakeholders who have engaged with and provide technology for testing, including but not limited to international and private sector partners;

(3) a list of tools, techniques, and procedures used by the Testing Center; and

(4) a list of critical maritime operational technologies examined by the Testing Center.

(e) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to carry out this section $2,000,000 for each of fiscal years 2023 through 2027."

Port Security Grant Program Cyber Funding

This proposal implements the recommendation to increase the cybersecurity funding in the Port Security Grant Program and Port Infrastructure Development Program.

A BILL

To establish a program within the United States Coast Guard to increase the cybersecurity funding in the Port Security Grant Program.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Sec. X Port Security Grant Program Cyber Funding

(a) Amendments.—

(1) Paragraph (a)(2)(C) of chapter 70103 of title 46, United States Code is amended by adding before the ".", "including a cybersecurity incident".

(2) Paragraph (b)(2) of chapter 70107 of title 46, United States Code is amended by adding after "security vessels,", "cybersecurity tools and assessments,".

(3) Chapter 70107 of title 46, United States Code is amended by adding at the end—

"(n) Cybersecurity activities.—Of the amounts made available for grants under this section for a given fiscal year, not less than 8 percent shall be used to make grants to improve the cybersecurity of ports."

Line-in; Line-out

46 U.S. Code § 70103 - Maritime transportation security plans

(a) National Maritime Transportation Security Plan.—

(1) The Secretary shall prepare a National Maritime Transportation Security Plan for deterring and responding to a transportation security incident.

(2) The National Maritime Transportation Security Plan shall provide for efficient, coordinated, and effective action to deter and minimize damage from a transportation security incident, and shall include the following:

(A) Assignment of duties and responsibilities among Federal departments and agencies and coordination with State and local governmental agencies.

(B) Identification of security resources.

(C) Procedures and techniques to be employed in deterring a national transportation security incident, including a cybersecurity incident.

46 U.S. Code § 70107 - Grants

(a) In general.—

…

(b) Eligible Costs.—The following costs of funding the correction of Coast Guard identified vulnerabilities in port security and ensuring compliance with Area Maritime Transportation Security Plans and facility security plans are eligible to be funded:

(1) Salary, benefits, overtime compensation, retirement contributions, and other costs of additional Coast Guard-mandated security personnel.

(2) The cost of acquisition, operation, and maintenance of security equipment or facilities to be used for security monitoring and recording, security gates and fencing, marine barriers for designated security zones, security-related lighting systems, remote surveillance, concealed video systems, security vessels, cybersecurity tools and assessments, and other security-related infrastructure or equipment that contributes to the overall security of passengers, cargo, or crewmembers. Grants awarded under this section may not be used to construct buildings or other physical facilities, except those which are constructed under terms and conditions consistent with the requirements under section 611(j)(8) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5196(j)(8)), including those facilities in support of this paragraph, and specifically approved by the Secretary. Costs eligible for funding under this paragraph may not exceed the greater of—

…

(n) Cybersecurity activities.—Of the amounts made available for grants under this section for a given fiscal year, not less than 8 percent shall be used to make grants to improve the cybersecurity of ports.

Port Infrastructure Development Program Cyber Funding

This proposal implements the recommendation to increase cybersecurity funding in the Port Infrastructure Development Program.

A BILL

To establish a program within the United States Coast Guard to Increased Funding for Cyber through the Port Infrastructure Development Program.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC.X. Increased Funding for Cyber through Port Infrastructure Development Program

(a) In General.—Section (c) of chapter 50302 of title 46, United States Code is amended as follows—

(1) in subparagraph (c)(3)(A)(ii) by adding "cybersecurity" after "improve the".

(2) in subparagraph (c)(7) by adding at the end—

"(D) Cybersecurity Activities.—Of the amounts made available for grants under this section for a given fiscal year, not less than 5 percent shall be used to make grants to improve the cybersecurity of ports."

Line-in; Line-out

(c) Port and Intermodal Improvement Program.—

(1) General authority.—Subject to the availability of appropriations, the Secretary of Transportation shall make grants, on a competitive basis, to eligible applicants to assist in funding eligible projects for the purpose of improving the safety, efficiency, or reliability of the movement of goods through ports and intermodal connections to ports.

(2) Eligible applicant.—The Secretary may make a grant under this subsection to the following:

(A) A State.

(B) A political subdivision of a State, or a local government.

(C) A public agency or publicly chartered authority established by 1 or more States.

(D) A special purpose district with a transportation function.

(E) An Indian Tribe (as defined in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304), without regard to capitalization), or a consortium of Indian Tribes.

(F) A multistate or multijurisdictional group of entities described in this paragraph.

(G) A lead entity described in subparagraph (A), (B), (C), (D), (E), or (F) jointly with a private entity or group of private entities.

(3) Eligible projects.—The Secretary may make a grant under this subsection—

(A) for a project, or package of projects, that—

(i) is either—

(I) within the boundary of a port; or

(II) outside the boundary of a port, but is directly related to port operations or to an intermodal connection to a port; and

(ii) will be used to improve the cybersecurity, safety, efficiency, or reliability of—

(I) the loading and unloading of goods at the port, such as for marine terminal equipment;

(II) the movement of goods into, out of, around, or within a port, such as for highway or rail infrastructure, intermodal facilities, freight intelligent transportation systems, and digital infrastructure systems; or

(III) environmental mitigation measures and operational improvements directly related to enhancing the efficiency of ports and intermodal connections to ports;

…

(7) Allocation of funds.—

(A) Geographic distribution.—Not more than 25 percent of the amounts made available for grants under this subsection for a fiscal year may be used to make grants for projects in any 1 State.

(B) Small projects.—The Secretary shall reserve 25 percent of the amounts made available for grants under this subsection each fiscal year to make grants for eligible projects described in paragraph (3)(A) that request the lesser of—

(i) 10 percent of the amounts made available for grants under this subsection for a fiscal year; or

(ii) $10,000,000.

(C) Development phase activities.—Not more than 10 percent of the amounts made available for grants under this subsection for a fiscal year may be used to make grants for development phase activities under paragraph (3)(B).

(D) Cybersecurity Activities.—Of the amounts made available for grants under this section for a given fiscal year, not less than 5 percent shall be used to make grants to improve the cybersecurity of ports.

Maritime Cyber Education and Certifications

This proposal implements the recommendation to create maritime cybersecurity education and certification programming at the United States Coast Guard.

A BILL

To establish a program within the United States Coast Guard to create maritime cybersecurity educational programs and a portable credential.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. X. MARITIME CYBER WORKFORCE EDUCATION AND CREDENTIALING PROGRAM

(a) AMENDMENTS.—In general chapter 701 of title 46, United States Code is amended—

(1) by adding at the end the following:

"SEC. 70126. MARITIME CYBER WORKFORCE EDUCATION AND CREDENTIALING PROGRAM

"(a) DEFINITIONS.—In this section:

"(1) COMMANDANT.—The term "commandant" means the Commandant of the United States Coast Guard.

"(2) PORTABLE CREDENTIAL.—The term "portable credential"—

"(A) means a documented award by a responsible and authorized entity that has determined that an individual has achieved specific learning outcomes relative to a given standard; and

"(B) includes a degree, diploma, license, certificate, badge, and professional or industry certification that—

"(i) has value locally and nationally in labor markets, educational systems, or other contexts;

"(ii) is defined publicly in such a way that allows educators, employers, and other individuals and entities to understand and verify the full set of skills represented by the credential; and

"(iii) enables a holder of the credential to move vertically and horizontally within and across training and education systems for the attainment of other credentials.

"(b) MARITIME TRANSPORTATION SECTOR-SPECIFIC CYBERSECURITY EDUCATIONAL RESOURCES.— Not later than one year after the passage of this act, the Commandant—in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, the Director of the National Initiative for Cybersecurity Education, and Administrators of the Federal Service Academies—shall compile and publish a compendium of educational resources focused on cybersecurity for the maritime transportation sector.

"(1) Periodic Update.—The compendium shall be reviewed and updated not less often than every 12 months after the initial publication of the compendium as outlined in section (b).

"(c) Portable Credential Program.—

"(1) IN GENERAL.—Not later than one year following the passage of this act, the Commandant, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Initiative for Cybersecurity Education, shall establish a program within the National Maritime Center to provide general and system-specific cyber educational programs for maritime workers through virtual platforms for coursework and training and hands-on skills labs and assessments, and provide a portable credential to individuals who achieve completion of coursework associated with the program.

"(d) Report on Public-Private Maritime Cyber Workforce Rotational Program.—

"(1) IN GENERAL.—Not later than one year following the passage of this act, the Commandant, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Initiative for Cybersecurity Education, submit a report to relevant Congressional committees assessing the feasibility of creating a public-private rotational program for cyber workforce positions within the United States Coast Guard.

"(2) REPORT REQUIREMENTS.—At a minimum, the report submitted to Congress pursuant to subparagraph (1) shall—

"(A) identify United States Coast Guard positions eligible for inclusion in the program;

"(B) propose criteria for private sector participation in the program; and

"(C) provide a legal assessment of the viability of the program under existing statute and authorities."

Endnotes

1. U.S. Department of Transportation, Maritime Administration, "Maritime Transportation System (MTS) Improving the U.S. Marine Transportation System," January 8, 2021. (https://www.maritime.dot.gov/outreach/maritime-transportation-system-mts/maritime-transportation-system-mts)

2. Maritime Transportation System Information Sharing and Analysis Center, "MTS-ISAC 2022 Annual Report," March 3, 2023, page 13. (https://www.mtsisac.org/post/mts-isac-publishes-2022-annual-report)

3. William Loomis, Virpratap Vikram Singh, Dr. Gary C. Kessler, and Dr. Xavier Bellekens, "Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity," *Atlantic Council*, October 4, 2021. (https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity)

4. The White House, "National Maritime Cybersecurity Plan to the National Strategy for Maritime Security," December 2020, page 1. (https://www.hsdl.org/c/abstract/?docid=848704)

5. U.S. Coast Guard, "Posture Statement 2023 Budget Overview," accessed on March 17, 2023, page 5. (https://www.uscg.mil/Portals/0/documents/budget/2023/FY%202023%20Posture%20Statement.pdf?ver=nSIvAr6imO5IsOC3m0PMsg%3D%3D&timestamp=1648484300591)

6. Office for Coastal Management, "Ports," March 15, 2023. (https://coast.noaa.gov/states/fast-facts/ports.html)

7. The Port of Los Angeles, "Port of Los Angeles Launches First-of-its-King Cyber Resilience Center," January 24, 2022. (https://www.portoflosangeles.org/references/2022-news-releases/news_012422_csc_ibm)

8. William Loomis, Virpratap Vikram Singh, Dr. Gary C. Kessler, and Dr. Xavier Bellekens, "Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity," *Atlantic Council*, October 4, 2021. (https://www.atlanticcouncil.org/in-depth-research-reports/report/raising-the-colors-signaling-for-cooperation-on-maritime-cybersecurity)

9. Ibid.

10. U.S. Coast Guard, "Posture Statement 2023 Budget Overview," accessed on March 17, 2023, page 5. (https://www.uscg.mil/Portals/0/documents/budget/2023/FY%202023%20Posture%20Statement.pdf?ver=nSIvAr6imO5IsOC3m0PMsg%3D%3D&timestamp=1648484300591)

11. Scott Disavino, "U.S. poised to regain crown as world's top LNG exporter," *Reuters*, January 4, 2023. (https://www.reuters.com/business/energy/us-poised-regain-crown-worlds-top-lng-exporter-2023-01-04)

12. G. James Herrera and Hibbah Kaileh, "Defense Primer: United States Transportation Command," *Congressional Research Service,* March 31, 2020, page 1. (https://crsreports.congress.gov/product/pdf/IF/IF11479/3)

13. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018. (https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world)

14. "Marine Firm James Fisher Reports Cyber Breach," *Reuters*, November 5, 2019. (https://www.reuters.com/article/us-james-fisher-cybercrime-idUSKBN1XF1SQ)

15. Marcus Hand, "MSC Confirms Malware Attack Caused Website Outage," *Seatrade Maritime News*, April 17, 2020. (https://www.seatrade-maritime.com/containers/msc-confirms-malware-attack-caused-website-outage)

16. Sean Lyngaas, "Hackers Breached Computer Network at Key US Port but Did Not Disrupt Operations," *CNN*, September 23, 2021. (https://www.cnn.com/2021/09/23/politics/suspected-foreign-hack-houston/index.html)

17. Adam Janofsky, "String of Cyberattacks on European Oil and Chemical Sectors Likely Not Coordinated, Officials Say," *The Record*, February 3, 2022. (https://therecord.media/string-of-cyberattacks-on-european-oil-and-chemical-sectors-likely-not-coordinated-officials-say)

18. Rowan Staden-Coats and Eklavya Gupte, "Cyberattack Causes Chaos at Key European Oil Terminals," *S&P Global*, February 2, 2022. (https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/oil/020322-cyberattack-causes-chaos-at-key-european-oil-terminals)

19. Jonathan Grieg, "Port of Lisbon Website Still Down as LockBit Gang Claims Cyberattack," *The Record*, December 29, 2022. (https://therecord.media/port-of-lisbon-website-still-down-as-lockbit-gang-claims-cyberattac)

20. Bill Toulas, "LockBit Ransomware Claims Attack on Port of Lisbon in Portugal," *Bleeping Computer*, December 30, 2022. (https://www.bleepingcomputer.com/news/security/lockbit-ransomware-claims-attack-on-port-of-lisbon-in-portugal)

21. Carly Page, "Maritime Giant DNV Says 1,000 Ships Affected By Ransomware Attack," *TechCrunch*, January 18, 2023. (https://techcrunch.com/2023/01/18/dnv-norway-shipping-ransomware)

22. Jonathan Greig, "Ransomware Attack on Maritime Software Impacts 1,000 Ships," *The Record*, January 16, 2023. (https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships)

23. DNV, Press Release, "Cyber-attack on ShipManager Servers – Update," January 23, 2023. (https://www.dnv.com/news/cyber-attack-on-shipmanager-servers-update-237931)

24. The White House, Press Release, "Presidential Policy Directive – Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil); Pub. L. 117-263, 136 Stat. 3659, 6 U.S.C. §651(5). (http://uscode.house.gov/view.xhtml?req=(title:6%20section:651%20edition:prelim)%20OR%20(granuleid:USC-prelim-title6-section651)&f=treesort&num=0&edition=prelim#). After enactment of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Sector-Specific Agencies became known as Sector Risk Management Agencies. See: William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4768, 6 U.S.C. §9002(a)(7). (https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf)

25. James M. Inhofe National Defense Authorization Act for Fiscal Year 2023, Pub. L. 117-263, 136 Stat. 3660, 6 U.S.C §665d. (http://uscode.house.gov/view.xhtml?req=(title:6%20section:665d%20edition:prelim)

26. U.S. Coast Guard, "Cyber Strategic Outlook," August 2021, pages 5 and 12. (https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf)

27. U.S. Committee on the Marine Transportation System, "What We Do," accessed on March 17, 2023. (https://www.cmts.gov/about-us)

28. U.S. Department of Homeland Security, Office of the Press Secretary, "Protecting America's Ports: Maritime Transportation Security Act of 2002," July 1, 2003, page 5. (https://www.aapa-ports.org/files/pdfs/mtsa_press_kit.pdf); Maritime Transportation Security Act, Pub. L. 107-295, 116 Stat. 2064, 46 U.S.C. §2101. (https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf)

29. FAA Reauthorization Act of 2018, Pub. L. 115-254, 132 Stat. 3186. (https://www.congress.gov/115/plaws/publ254/PLAW-115publ254.pdf);

U.S. Coast Guard, "Navigation and Vessel Inspection Circular No. 01-20," February 26, 2020. (https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/5ps/NVIC/2020/NVIC_01-20_CyberRisk_dtd_2020-02-26.pdf?ver=2020-03-19-071814-023)

30. The initial inclusion of cybersecurity items in the required Facility Security Assessment and Facility Security Plan was due by October 1, 2022.

31. Coast Guard Maritime Commons, "Coast Guard Releases New Maritime Cybersecurity Assessment & Annex Guide," January 23, 2023. (https://mariners.coastguard.blog/2023/01/23/coast-guard-releases-new-maritime-cybersecurity-assessment-annex-guide); Coast Guard Maritime Commons, "NVIC 01-20, 'Guidelines for Addressing Cyber Risks at MTSA Regulated Facilities,'" March 25, 2020. (https://mariners.coastguard.blog/2020/03/25/nvic-01-20-guidelines-for-addressing-cyber-risks-at-mtsa-regulated-facilities)

32. Vincent Milano, "National Maritime Cybersecurity Plan Released," *Homeland Security Digital Library*, January 12, 2021. (https://www.hsdl.org/c/national-maritime-cybersecurity-plan-released)

33. U.S. Coast Guard, Press Release, "U.S. Coast Guard Addresses Threats to National Security in Updated Cyber Strategic Outlook," August 3, 2021. (https://content.govdelivery.com/accounts/USDHSCG/bulletins/2eaafce); U.S. Coast Guard, "Cyber Strategic Outlook," August 2021. (https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf)

34. U.S. Coast Guard, "Cyber Strategic Outlook," August 2021, page 7. (https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf)

35. U.S. Coast Guard, "Cyber Strategy," June 2015, page 33. (https://www.dco.uscg.mil/Portals/10/Cyber/Docs/CG_Cyber_Strategy.pdf?ver=nejX4g9gQdBG29cX1HwFdA%3D%3D)

36. U.S. Coast Guard, "Cyber Strategic Outlook," August 2021, page 28. (https://www.uscg.mil/Portals/0/Images/cyber/2021-Cyber-Strategic-Outlook.pdf)

37. U.S. Coast Guard, "United States Coast Guard Strategy," October 2022, page 12. (https://media.defense.gov/2022/Oct/12/2003094294/-1/-1/0/USCG-STRATEGY-2022.PDF)

38. U.S. Coast Guard, "Ready Workforce 2030," April 2022, page 21. (https://media.defense.gov/2022/May/11/2002994521/-1/-1/0/READY%20WORKFORCE%202030%20OUTLOOK.PDF). There are additional USCG efforts in workforce development, such as the Direct Commission Cyber Officer program, introduced in September 2021, and a cyber mission specialist rating that would allow enlisted members to pursue opportunities in Cyberspace Operations, which is expected to be available in 2023. The new rating provides an attractive option for rotational programs for non-commissioned personnel. For more information, see: Kathy Murray, "New direct commissioning for Coast Guard cyber officers offers new opportunities to serve," *U.S. Coast Guard*, January 14, 2022. (https://www.mycg.uscg.mil/News/Article/2898718/new-direct-commissioning-for-coast-guard-cyber-officers-offers-new-opportunitie); and Kathy Murray, "New Cyber Mission Specialist Enlisted Rating Expands Cyberspace Career Opportunity," *U.S. Coast Guard*, February 7, 2022. (https://www.mycg.uscg.mil/News/Article/2924033/new-cyber-mission-specialist-enlisted-rating-expands-cyberspace-career-opportun)

39. U.S. Government Accountability Office, "Coast Guard: Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands," September 2022, page 14. (https://www.gao.gov/assets/gao-22-105208.pdf). Note: The USCG uses the manpower requirements determination model to link mission requirements with manpower requirements as outlined. See: "Manpower Requirements Determination (MRD)," *U.S. Coast Guard*, accessed on March 17, 2023. (https://www.dcms.uscg.mil/Portals/10/CG-1/cg1B/docs/MRD_brochure.pdf?ver=2017-03-27-152844-357)

40. U.S. Government Accountability Office, "Coast Guard: Workforce Planning Actions Needed to Address Growing Cyberspace Mission Demands," September 2022, page 14. (https://www.gao.gov/assets/gao-22-105208.pdf)

41. Ibid., page 28.

42. Cybersecurity and Infrastructure Security Agency and U.S. Coast Guard, "Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems," June 23, 2022. (https://www.cisa.gov/uscert/sites/default/files/publications/AA22-174A_Joint_CSA_Malicious_Cyber_Actors_Exploiting_Log4Shell_in_Unpatched_VMware_Horizon_Systems_FINAL.pdf)

43. Ibid., page 11.

44. Maritime Transportation System Information Sharing and Analysis Center, "MTS-ISAC 2022 Annual Report," March 3, 2023, page 2. (https://www.mtsisac.org/post/mts-isac-publishes-2022-annual-report)

45. "MTS-ISAC Services: Information Sharing," *Maritime Transportation System ISAC*, accessed March 17, 2023. (https://www.mtsisac.org/services)

46. Department of Homeland Security, Press Release, "DHS Announces New Cybersecurity Performance Goals For Critical Infrastructure," October 27, 2022. (https://www.dhs.gov/news/2022/10/27/dhs-announces-new-cybersecurity-performance-goals-critical-infrastructure)

47. The White House, Press Release. "National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems," July 28, 2021. (https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems)

48. Cybersecurity and Infrastructure Security Agency, "CISA Welcomes Input on New Cyber Incident Reporting Requirements," September 9, 2022. (See archived version at: https://web.archive.org/web/20221102112842/https://www.cisa.gov/news/2022/09/09/cisa-welcomes-input-new-cyber-incident-reporting-requirements)

49. United States Coast Guard, "Posture Statement 2023 Budget Overview," accessed on March 17, 2023, page 32. (https://www.uscg.mil/Portals/0/documents/budget/2023/FY%202023%20Posture%20Statement.pdf?ver=nSIvAr6imO5IsOC3m0PMsg%3D%3D&timestamp=1648484300591)

50. U.S. Department of Homeland Security, "FY2023 Budget in Brief," March 22, 2022, page 53. (https://www.dhs.gov/sites/default/files/2022-03/22-%201835%20-%20FY%202023%20Budget%20in%20Brief%20FINAL%20with%20Cover_Remediated.pdf); U.S. Department of Homeland Security, "U.S. Coast Guard Budget Overview, Fiscal Year 2023 Congressional Justification," accessed March 17, 2023, page 307. (https://www.dhs.gov/sites/default/files/2022-03/U.S.%20Coast%20Guard_Remediated.pdf)

51. "CyTRICS Cyber Testing for Resilient Industrial Control Systems," *U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response*, accessed on March 17, 2023. (https://cytrics.inl.gov)

52. "NISAC Performers and Projects," *U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency*, March 2022. (https://www.cisa.gov/nisac-projects)

53. "Bipartisan Infrastructure Law: Maritime Administration," *U.S. Department of Transportation, Maritime Administration*, October 20, 2022. (https://www.maritime.dot.gov/about-us/bipartisan-infrastructure-law-maritime-administration)

54. "About Port Infrastructure Development Grants," *U.S. Department of Transportation, Maritime Administration*, February 2, 2023. (https://www.maritime.dot.gov/PIDPgrants)

55. U.S. Department of Homeland Security, Press Release, "DHS Announces Funding Allocations for FY 2022 Preparedness Grants," August 17, 2022. (https://www.dhs.gov/news/2022/08/17/dhs-announces-funding-allocations-fy-2022-preparedness-grants)

56. U.S. Department of Homeland Security, Federal Emergency Management Agency, "Fiscal Year 2022 Port Security Grant Program Fact Sheet," May 13, 2022. (https://www.fema.gov/fact-sheet/fiscal-year-2022-port-security-grant-program-fact-sheet)

57. U.S. Department of Homeland Security, Press Release, "DHS Announces Funding Allocations for FY 2022 Preparedness Grants," August 17, 2022. (https://www.dhs.gov/news/2022/08/17/dhs-announces-funding-allocations-fy-2022-preparedness-grants)

58. Minimum spending requirement percentages are based on author interview with industry expert on January 26, 2023.

About the Authors

Jiwon Ma is a program analyst at FDD's Center on Cyber and Technology Innovation, where she contributes to the CSC 2.0 project. She has contributed to cybersecurity reports published by Columbia University's School of International and Public Affairs (SIPA) and by the Belfer Center for Science and International Affairs. Jiwon received a Master of International Affairs degree from SIPA and a BA in global studies from Lesley University.

Will Loomis is an associate director with the Atlantic Council's Cyber Statecraft Initiative under the Digital Forensic Research Lab (DFRLab). In this role, he manages a wide range of projects at the nexus of geopolitics and national security with cyberspace, including leading the team's work on critical infrastructure cybersecurity.

ACKNOWLEDGEMENTS

The authors would like to thank Sean Plankey, Scott Dickerson, Rear Admiral Wayne Arguin, Captain Andrew Meyers, and Virpratap Vikram Singh for having interviews with the authors, reviewing the report, and providing feedback. We are grateful for the willingness of the CSC 2.0 co-chairs, distinguished advisors, and senior advisors to share expertise and offer advice on this report. We are also grateful to Annie Fixler, David Adesnik, Erin Blumenthal, David May, Daniel Ackerman, and Miriam Himmelfarb for bringing this report to life.

Cover Photo: Port of Los Angeles on April 15, 2022, in San Pedro, California. (Photo by Qian Weizhong/VCG via Getty Images)

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Michael "Mike" J. Gallagher, U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Thomas A. "Tom" Fanning, Chairman, President, and Chief Executive Officer of Southern Company

James R. "Jim" Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

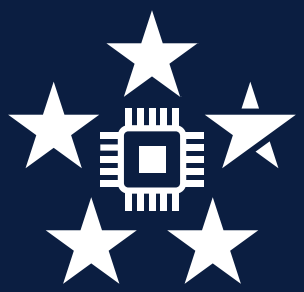
Samantha F. Ravich, Chair of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Benjamin E. "Ben" Sasse, Former U.S. Senator for Nebraska

Suzanne E. Spaulding, Senior Adviser for Homeland Security at the Center for Strategic and International Studies

Partner

FDD



CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission