CSC 2.0

March 2025

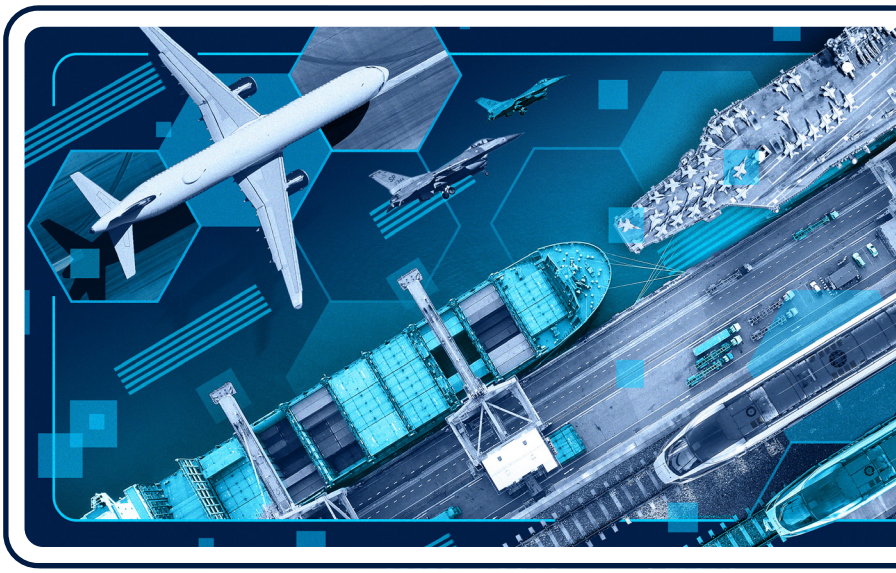
Military Mobility Depends on Secure Critical Infrastructure

By Annie Fixler, RADM (Ret.) Mark Montgomery, and Rory Lane

Table of Contents

Executive Summary

A direct military engagement between the United States and a near-peer adversary would require the swift mobilization and deployment of a sizable U.S. military force. Moving troops and equipment efficiently over land, sea, and air is essential to America's ability to project power, support partners and allies, and sustain forces to fight and win wars. Alongside the U.S. military's own assets, commercially owned and operated critical infrastructure enables this military mobility. While U.S. Transportation Command (TRANSCOM) conducts logistical operations to facilitate the mobility of U.S. forces, civilian-owned rail networks, commercial ports, and airport authorities will handle transportation of the majority of servicemembers and materiel during a significant, rapid mobilization.



An FDD design collage featuring from left to right: a U.S. Navy aircraft carrier (pigphoto via Getty Images), an F-16 Fighting Falcon fighter (Harald Tittel/picture alliance via Getty Images), a narrow body aircraft (Thiago B Trevisan via Shutterstock), a shipping port (Travel mania via Shutterstock), and passenger trains (Clare Louise Jackson via Shutterstock)

U.S. adversaries know that compromising this critical infrastructure through cyber and physical attacks would impede America's ability to deploy, supply, and sustain large forces. As the U.S. intelligence community's 2024 annual threat assessment warned, China would "consider aggressive cyber operations against U.S. critical infrastructure and military assets" in the event of an imminent conflict with the United States. Beijing would seek to use these operations not only as a deterrent against further U.S. military action but also specifically to "interfere with the deployment of U.S. forces."[1]

Over the past year, the intelligence community has revealed how deeply Chinese hackers known as Volt Typhoon penetrated U.S. transportation, energy, and water systems.[2] Volt Typhoon demonstrated China's capability to gain and maintain persistent access to closed systems and pre-position malicious payloads to cause disruption and destruction.[3] Meanwhile, other Chinese Communist Party (CCP) malicious cyber operations, including Flax Typhoon, hijacked cameras and routers, and Salt Typhoon burrowed deep into U.S. telecommunications networks.[4] In addition to enabling potential disruption, compromising critical infrastructure allows Beijing to amass information about the movement of goods, surreptitiously watching as the United States moves its military equipment across the country. Given these threats, the U.S. military has a vested interest in the security of the nation's critical transportation infrastructure.

The cybersecurity of the critical air, rail, and maritime infrastructure that underpins U.S. military mobility is insufficient.[5] To improve resilience, the United States needs significant investment by the government and private sector as well as improved public-private collaboration. The nation can no longer afford to waste time debating the immediacy of the threat. Washington must identify and resource solutions now.

Organization of Critical Infrastructure and Defense Critical Infrastructure

Under current U.S. policy, Washington has two distinct designations for national "critical infrastructure" and "defense critical infrastructure." The U.S. government recognizes 16 critical infrastructure sectors and assigns each a federal agency partner, known as a sector risk management agency (SRMA).[6] A 2013 presidential policy directive established this classification, and an April 2024 national security memorandum reaffirmed it.[7] While some federal agencies that serve as SRMAs are also regulators, the responsibilities are separate and unique.

The Department of Defense (DoD), meanwhile, recognizes 10 defense infrastructure sectors. DoD first defined them in 2005 and designated a Defense Infrastructure Sector Lead Agent (DISLA) to interact with each.[8] While the lead-agent designation has since been retired with the incorporation of defense critical infrastructure protection into DoD's Mission Assurance Strategy,[9] the term DISLA is still useful for describing agencies' roles, responsibilities, and authorities related to different types of critical infrastructure.

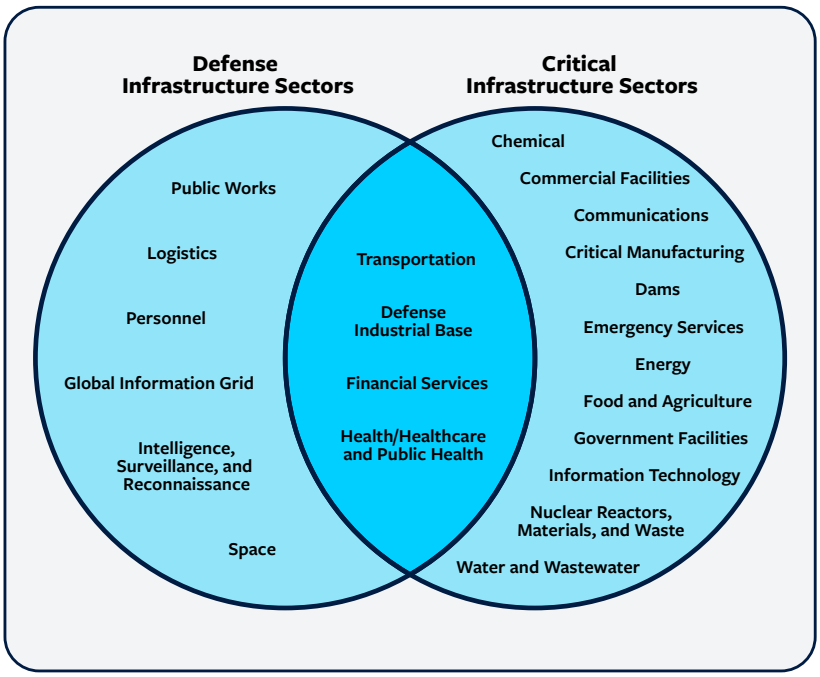
TRANSCOM was the DISLA responsible for identifying and safeguarding defense critical infrastructure within the transportation sector. Within TRANSCOM, Air Mobility Command is the Air Force component responsible for conducting aerial transportation and airlift. Military Surface Deployment and Distribution Command is the Army component charged with managing the intermodal connections to the nation's strategic seaports and facilitating surface transportation via road and rail. Military Sealift Command is the Navy component that conducts sealift, the transportation of materiel in the maritime domain.

Across all defense critical infrastructure sectors, the DISLAs work directly with military commands and mission owners to identify the task-critical assets required to maintain mission-essential functions,[11] the most important of which are designated as defense critical assets. The destruction or disruption of a defense critical asset would seriously impact DoD missions. DoD's Defense Critical Infrastructure Program has therefore sought to identify, label, and mitigate risks to such infrastructure.

This work, however, has been siloed from efforts by other federal agencies to identify and manage risk and secure critical infrastructure in their roles as SRMAs. The National Infrastructure Protection Plan, which outlines whole-of-government and public-private efforts to manage natural and man-made risks to critical infrastructure, does not acknowledge the intersection of national critical infrastructure and defense critical infrastructure. Similarly, as codified in the Fiscal Year 2021 National Defense Authorization Act, SRMAs are responsible for facilitating information sharing between their sector and other federal agencies, including the Department of Homeland Security — but not DoD.[12]

The April 2024 national security memorandum on critical infrastructure security (known as NSM-22) expressly acknowledged this gap and took a long-overdue first step to address it. In addition to reaffirming the role of SRMAs, NSM-22 tasked SRMAs with incorporating defense critical infrastructure (and other national priorities) into their existing sector risk management responsibilities.[13] The memorandum also instructed DoD to work with the SRMAs and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) to evaluate sector-specific risks and provide advice on prioritized mitigations to SRMAs in order to strengthen the security and resilience of defense critical infrastructure. Still, challenges persist across multiple critical infrastructure sectors, most urgently (for military mobility) in the maritime, aviation, and rail subsectors.

Figure 1: Defense Infrastructure Sectors vs. National Critical Infrastructure[10]



Maritime Mobilization Infrastructure

Each year, about 1.5 billion tons of goods, valued at over $2 trillion, transit U.S. seaports.[14] The U.S. ports, vessels, and other assets that comprise the maritime transportation system subsector are vital not only to commercial trade but also to the U.S. military's ability to deploy forces overseas.[15] "More than 90 percent of the equipment and supplies used by U.S. warfighters travels by sea," according to Military Sealift Command.[16] Any large deployment of U.S. troops would certainly be accompanied by a major sealift effort.

There are two categories of sealift — surge and sustainment. The former supports initial movements of troops, equipment, and supplies to satisfy time-critical war fighting requirements, while the latter provides continuous support to previously deployed forces over an extended period.[17] Surge sealift capacity is largely maintained by the U.S. Maritime Administration (MARAD) within the Department of Transportation (DOT).[18] Despite its separation from DoD, MARAD works closely with Military Sealift Command to maintain sealift readiness and protect the strategic seaports that would be used during mobilization and sustainment operations.[19]

Scholars and policymakers have raised concerns, however, that neither Military Sealift Command nor MARAD maintains a sufficient fleet to meet surge capacity needs in the event of a conflict with China. While Military Sealift Command is responsible for resupplying naval ships and strategically pre-positioning and moving military cargo, its surge sealift fleet has only about 15 ships. MARAD also has about 50 ships for this purpose.[20] In a February 2024 letter to the heads of TRANSCOM and MARAD, Rep. Mike Gallagher (R-WI), then chairman of the House Select Committee on the Chinese Communist Party, called the U.S. government's sealift fleet "woefully inadequate."[21] MARAD contracts with commercial shipping companies,[22] but Gallagher warned that the U.S. merchant fleet available for this purpose is also too small. While an assessment of U.S. sealift capacity requirements is beyond the scope of this paper, the nation's lack of excess sealift capacity means that the U.S. military's ability to mobilize forces could be severely degraded by any cyber or physical incident impacting the availability of government-owned or commercial vessels.

Civilian-owned maritime infrastructure plays an even more crucial role in sealift than the government-owned and chartered commercial vessels that will conduct it. In addition to six military ports, TRANSCOM designates 18 commercially owned ports as strategic seaports, including major hubs such as the ports of Long Beach, Corpus Christi, Savannah, and Guam. These are "vital nodes of the nation's transportation infrastructure that play a critical role in DoD's ability to deploy forces and equipment worldwide," RADM Derek Trinque, director for strategic plans, policy, and logistics for TRANSCOM, explained at a House Homeland Security subcommittee hearing in February 2024.[23]

As Trinque explained, all the commercial strategic seaports have readiness plans so that the facilities — including the docks, staging areas, and rail yards — can be turned over to DoD within 48 hours if necessary. Participation in the strategic seaport program is voluntary. Nine federal agencies, including MARAD, the U.S. Coast Guard, and Military Sealift Command, come together to ensure the readiness of these strategic seaports and 14 additional alternative ports (13 commercial and one military port).[24] These 31 commercial ports and all other ports around the country have a U.S. Coast Guard captain of the port responsible for their safe and secure operation.[25]

At that same hearing, RADM John Vann, commander of Coast Guard Cyber Command, warned about cyber threats to the maritime transportation system. The system's "size, interdependence, complexity, and criticality" make "it a prime target for criminals, activists, terrorists, state-sponsored actors, and adversarial nation states," Vann said. He added, "A successful cyberattack could impose unrecoverable losses to port operations and electronically stored information, hampering national economic activity, and disrupting global supply chains."[26]

Prior disruptions caused by non-cyber incidents provide a glimpse of the potential impact of a cyberattack. Significant interruptions of normal port operations lead the cost of goods to rise, hurting the economy.[27] Such "knock-on effects" were acutely felt during the COVID-19 pandemic, with container imports across U.S. ports declining by 7 percent in the first half of 2020.[28] Past closures of major U.S. ports as a result of labor disputes have caused "billions of dollars in losses" and contributed to supply-chain disruptions, according to an April 2023 Business Journal report.[29]

Recognizing this threat, the Biden administration took a series of steps in February 2024 to bolster the maritime transportation system's cyber defenses.[30] First, the administration issued an executive order clarifying that the security authorities and responsibilities of Coast Guard captains of the port extend to the realm of cyberspace. The administration further clarified

that owners, agents, or operators of vessels and ports must report cybersecurity incidents to the FBI, CISA, and captains of the port.[31] The administration also announced that the Coast Guard would develop minimum cybersecurity requirements for the maritime transportation system as well as cyber risk management actions to mitigate risks from "foreign adversarial technological, physical, and cyber influence."[32] While these requirements are deemed to be sensitive and will not be released publicly, captains of the port are using them to work directly with critical infrastructure owners and operators to implement the directives.[33]

A year later, in January 2025, the Coast Guard issued a final rule establishing minimum cybersecurity requirements for U.S.-flagged vessels and ports.[34] The rule will go into effect in July 2025, requiring regulated entities to implement basic cybersecurity controls, develop incident response plans, conduct annual audits, and report cyber incidents to the U.S. government.

A specific concern is the prevalence of Chinese-made automated equipment at numerous U.S. ports, potentially providing CCP hackers with opportunities for cyber-espionage or disruptive attacks.[35] In February 2024, MARAD released a U.S. Maritime Advisory calling out the threat posed by port equipment and technologies sourced from adversarial foreign nations. The advisory specifically mentioned security inspection equipment from Chinese company Nuctech; the LOGINK logistics management platform, developed and promoted by China's Ministry of Transportation; and ship-to-shore cranes manufactured by Shanghai Zhenhua Heavy Industries Company Limited (ZPMC). MARAD warned that Nuctech's poor-quality equipment "impairs U.S. efforts to counter illicit international trafficking in nuclear and other radioactive materials" and that LOGINK "very likely provides" Beijing with "access to and/or collection of sensitive logistics data." The advisory further warned malign actors could remotely operate ZPMC cranes.[36]

In a subsequent study on ZPMC, MARAD reported that Coast Guard cyber teams assessed the security of 92 ZPMC cranes and did not find malicious or suspicious code indicative of CCP malfeasance. They did, however, find several known cybersecurity vulnerabilities.[37] Such vulnerabilities are not unusual, but malicious actors could exploit them to compromise the safety and security of these cranes or disrupt their efficient operation, but the Coast Guard found no evidence that Beijing pre-positioned vulnerabilities in the cranes.

On the specific issue of ZPMC and military mobility, Trinque noted that while strategic seaports do have ZPMC cranes on-premises, the military can use other equipment when it deploys from those ports. "Our current assessment is none of our strategic seaports right now are wholly dependent on those cranes," he testified to Congress.[38] Trinque's remarks, however, may undersell the national and economic security threat posed by an adversary-owned company that controls 80 percent of all cranes in use at U.S. ports across the country.[39]

Indeed, a September 2024 joint report by the House Select Committee on the Chinese Communist Party and the House Homeland Security Committee warned that the subsector is "dangerously reliant on equipment and technology that has been produced, manufactured, assembled, or installed" in China.[40] While commercial port operators dismissed some concerns about ZPMC cranes, noting that critical component parts come from Western firms, the report details that these Western companies ship the parts to China, where they are stored for up to 18 months near a Chinese naval base. ZPMC engineers install the parts on the cranes "without oversight from the original manufacturer." The report noted that in the specific case of Swiss company ABB, the company provides ZPMC "with design schematics, which would allow ZPMC to create a backdoor in the hardware."[41]

The joint report further detailed instances in which ZPMC cranes contained unauthorized cellular modems that collect data on equipment usage. The port operators did not request the inclusion of this equipment as part of their purchase agreements and, in some cases, had expressly declined this feature. But ZPMC installed the modems anyway, creating — in the committees' words — "an obscure method to collect information, and bypass firewalls in a manner that could potentially disrupt port operations."[42] Furthermore, China's ability to demand access to ZPMC's software means that Beijing could manipulate the systems or use them to amass information for espionage purposes.[43]

Two months later, in November 2024, the U.S. Coast Guard issued an updated directive regarding the cyber risks posed by Chinese-made ship-to-shore cranes.[44] "By design, these cranes may be controlled, serviced, and programmed from remote locations," the Coast Guard warned, "and those features potentially leave STS cranes manufactured by PRC companies vulnerable to exploitation, threatening the maritime elements of the national transportation system."[45] The directive is not available publicly,

but the Coast Guard required all owners and operators of Chinese ship-to-shore cranes to get a copy from their captain of the port or district commander.

Despite the Biden administration's rhetorical focus on maritime cybersecurity, the Coast Guard's FY 2025 budget requested no additional funding from Congress to support SRMA activities. In fact, the Coast Guard has no funding specifically designated for work with the private sector to improve the cyber resiliency of America's port infrastructure.[46] The Trump administration has not yet released its FY 2026 budget, so it remains to be seen whether it will address its predecessor's shortcomings in this area.

Aviation Industry's Role in Mobilization

The U.S. aviation subsector is a vital transportation artery that moves millions of tons of freight and over 1 billion passengers annually.[47] The smooth operation of the thousands of aircraft and hundreds of major airports that make up this industry relies on a diverse set of digital and cyber-physical systems, including security scanning equipment, customer-facing reservation systems, networked avionics and navigation equipment, and air traffic control systems. The subsector includes commercial airlines, general aviation activities, air cargo shipments, and airports. These primary components are further supported by a diverse set of vendors providing aviation support functions such as maintenance, flight planning, and other services. This complex network presents a wide attack surface for cyber-threat actors hoping to disrupt U.S. aviation infrastructure and transportation networks. As the DOT's assistant inspector general for aviation audits warned in 2017, "Cyber-based threats—from both internal and external sources—are rapidly evolving and could threaten the connectivity of an increasingly complex aviation infrastructure."[48]

For example, in November 2022, a cyberattack against flight-planning software company Jeppesen, a Boeing subsidiary, temporarily disrupted the receipt and processing of Notice to Air Missions (NOTAM) alerts through its platform.[49] NOTAM provides advanced information to pilots about potential hazards along their routes. Three months later, a misconfigured file knocked the NOTAM system offline. The Federal Aviation Administration (FAA) halted departures for over an hour while addressing the outage. Over 1,300 flights were canceled, and another 9,000 were delayed.[50] In July 2024, a broken software update from cybersecurity firm CrowdStrike caused chaos and thousands of canceled flights across the globe.[51] Although a computer glitch and a faulty update (not cyberattacks) caused the latter two massive disruptions, they reveal inherent vulnerabilities in the highly interconnected network of information systems that facilitate air travel.[52]

The FAA is charged with managing the critical air traffic control systems that allow this transportation network to function. This collection of systems is known as the U.S. National Airspace System (NAS). "Cybersecurity breaches" in this system "can have significant physical and consequential impacts," warned a 2021 report by the DOT's Office of the Inspector General.[53]

Because many elements of the NAS have shared military functions — with the FAA also managing DoD flights over U.S. airspace[54] — a cyberattack on the NAS could impact a U.S. military mobilization effort.[55] Compromising critical components of the NAS could disrupt the coordination of military flights, delay critical deployments, or even lead to the exposure of sensitive military operational plans. The reliance on legacy systems within the NAS exacerbates these risks, as older technologies are not equipped to repel the sophisticated cyberattacks that adversaries can deploy today.

Indeed, a September 2024 Government Accountability Office (GAO) report warned that an overwhelming majority of air traffic control systems are dangerously out-of-date.[56] While the

Cybersecurity breaches of the National Airspace System can have significant physical impacts, but an overwhelming majority of air traffic control systems are dangerously out-of-date, warned the GAO.

FAA has ongoing modernization plans, the implementation has often been slow, has not prioritized the most critical systems, has faced budget shortfalls, and has lacked oversight, the GAO warned. Kevin Walsh, director of information technology and cybersecurity at the GAO, reiterated these concerns in testimony before the Senate Committee on Commerce, Science, and Transportation in December, noting that the FAA's modernization efforts have had mixed results at best, with the FAA acting far too slowly "to modernize the most critical and at-risk systems."[57]

The lack of prioritization of critical systems reflects the FAA's broader failure to properly categorize safety-critical information systems. Until recently, according to the 2021 inspector general report, the FAA consistently miscategorized systems as low or moderate rather than high impact, failing to recognize how severe a system failure would be. The report succinctly noted that even once the FAA had begun properly categorizing systems, it was using an outdated metric to identify these systems and lacked formal processes for implementing security controls. In short, the FAA had "not yet mitigated the risk that the NAS could be vulnerable to threats."[58]

At the same time, the FAA's own inspector general further cautioned that the FAA's efforts to modernize the NAS through implementing the Next Generation Air Transportation System (NextGen) may actually increase cybersecurity risk. NextGen is reliant on integrated information systems and satellite-based technologies.[59] If the FAA does not simultaneously improve its ability to recognize safety-critical information and systems, modernization will not result in increased cybersecurity.

Beyond the air traffic control systems, DoD also leverages civilian airports to rapidly and efficiently mobilize and deploy troops and materiel. As of 2022, DoD had agreements with 69 civilian airports to use their facilities.[60] The FAA works with DoD to ensure funding for the infrastructure at these airports that the military deems necessary. This funding, however, does not account for cybersecurity needs. The private or public airport operating authorities too often fail to view critical infrastructure cyber resilience as a requirement, leaving these airports vulnerable to cyberattack. In August 2024, for example, the Seattle-Tacoma Airport suffered a ransomware attack that disrupted internet and phone systems. Over the Labor Day travel weekend, gate agents had to handwrite boarding passes, and the luggage sorting system had to be operated manually. The criminal hackers claim to have stolen data from the Port of Seattle, the airport's operator.[61]

Air cargo service providers and commercial airlines themselves are also essential for supporting the U.S. military's capacity to conduct airlift for global force projection. As necessary, DoD will utilize commercial assets to supplement its own aircraft. TRANSCOM is authorized to activate elements of the Civil Reserve Air Fleet (CRAF), a voluntary group of nearly 30 U.S. air carriers, to provide airlift support for minor regional crises, humanitarian assistance, disaster relief efforts, major theater war, and periods of national mobilization.[62]

Historically, CRAF has been activated three times — first in support of operations Desert Shield and Desert Storm from 1990 to 1991, then in support of Operation Iraqi Freedom from 2002 to 2003, and finally in support of the U.S. evacuation from Afghanistan in 2021.[63] Support for a national mobilization effort represents the highest level at which CRAF can be activated. A tier 3 activation of CRAF would utilize significant numbers of commercial aircraft to provide surge airlift support in the event of a "national-defense related emergency or war."[64]

There is limited public discussion and evaluation of the potential disruptive impact of cyberattacks against CRAF carriers. There have also been few examples of deliberate cyberattacks against active commercial flights. Modern aircraft, however, are highly networked entities that the FAA refers to as "e-enabled aircraft."[65] Networked functions on e-enabled aircraft include avionics instruments, weather and navigation systems, air traffic control functions, and passenger safety systems. These, in turn, provide attack vectors for adversaries looking to disrupt the safe operation of U.S. aircraft.[66]

To begin addressing the range of vulnerabilities affecting the subsector, the FAA in August 2024 announced proposed rulemaking on "airworthiness standards" covering airplanes, propellers, and aircraft engines. The proposed rule aims to prevent "intentional unauthorized electronic interactions" — that is, cyberattacks that could impact safety.[67] Recognizing that "[a]ircraft, engines, and propellers increasingly incorporate networked bus architectures susceptible to cybersecurity threats," the rule will cover a wide range of systems that provide control functions for aircraft. These include "propulsion controls, monitoring functions that track the health of the engine's systems, communication functions such as data buses and networks, and auxiliary equipment such as fuel, lube, or pneumatic subsystems with embedded electronics."[68]

The Transportation Security Administration (TSA), meanwhile, is responsible for securing the nation's transportation systems. In aviation, that includes security oversight of commercial air transport and airport security. As part of this mission, TSA has issued a series of cybersecurity-related emergency amendments (EAs) for the aviation subsector. The most recent EA,

issued in March 2023, requires airports and aircraft operators to segregate operational technology systems from information technology systems; implement access controls to prevent unauthorized access to critical systems; implement continuous monitoring and detection policies and procedures for cyberattacks or other anomalous activities; and update software with security patches in a timely manner using a risk-based methodology. TSA also requires regulated entities to report cybersecurity incidents to CISA, establish a cybersecurity point of contact to interface with TSA, create a cybersecurity incident response plan, and conduct cybersecurity vulnerability assessments.[69]

During a hearing before the Senate Commerce, Science, and Transportation Committee, Airlines for America's cybersecurity managing director, retired Brig. Gen. USAF Marty Reynolds, noted that there are ongoing challenges aligning cybersecurity regulatory requirements across the industry. In a hopeful note, he acknowledged that the FAA is using TSA's incident reporting process as part of its efforts. Reynolds also noted that his organization has been working with TSA to help the agency understand threat-based, risk-informed programs in the subsector.[70]

Despite the FAA's and TSA's belated efforts to improve the cybersecurity of the aviation subsector, the infrastructure remains vulnerable. Air route traffic control centers, radar sites, and airports, in particular, are attractive targets for actors seeking to disrupt CRAF activation and the ability to conduct safe flights over U.S. airspace.

The Railroads' Strategic Role

The U.S. military's ability to conduct airlift and sealift hinges on the nation's rail network. Since the May 2021 ransomware attack on Colonial Pipeline, TSA has accelerated efforts to regulate the cybersecurity of critical infrastructure for which it serves as SRMA, including freight and passenger rail. And yet, across the transportation sector, companies are too often making a "less than socially optimal level of cybersecurity investment," TSA cautioned in November 2024.[71] This is particularly concerning, as the U.S. intelligence community has warned that China can disrupt U.S. critical infrastructure, calling out rail systems in particular.[72]

Rail cybersecurity has become more essential in recent years as the industry has increasingly digitized to improve efficiency and safety. After a series of accidents, Congress required near-universal adoption by 2020 of positive train control (PTC).[73] PTC is an automated system designed to mitigate the danger posed by operator error and to prevent collisions and derailments caused by excessive speed. Across nearly 60,000 miles of track,[74] PTC sensors record data about the location, direction, and speed of locomotives operating on the same track, compare real-time data to detect unsafe operations, and automatically correct operator errors by communicating corrections back to the locomotive computer.[75] Beyond PTC itself, networked operational technology systems provide essential train control functions such as dispatching, communications and signals, and electric traction systems.[76] On a constant basis, remote trackside sensors communicate wirelessly to train control offices and central dispatches while a two-man crew operates most freight trains.[77]

The U.S. rail system is classified into two distinct categories: the freight rail system and the passenger rail system. The latter includes all intercity, commuter, metro, subway, and light-rail networks.[78] U.S. freight rail lines are privately owned and largely operated by a set of six major firms known as Class I railroads.[79] Strategic rail lines connect over 140 military bases and other defense installations to the nation's seaports and serve as the primary transport mode for containerized goods, ammunition, and large pieces of equipment, such as tanks and armored vehicles. While the U.S. military operates a government-owned fleet of approximately 1,350 railcars, 10,000 shipping containers, and 1,850 heavy-duty flat cars,[80] this fleet must travel over privately owned rail lines. Commercial freight providers are also a necessary supplement in any U.S. mobilization effort.[81]

More than 40,000 miles of track are essential to the movement of servicemembers and military equipment. Surface Deployment and Distribution Command (SDDC) — the TRANSCOM component charged with identifying DoD requirements for transporting materiel via the domestic U.S. rail system[82] — designates these 40,000 miles as the Strategic Rail Corridor Network (STRACNET).[83] By mileage, STRACNET represents about a third of the entire U.S. rail network. In partnership with the Federal Railroad Administration (FRA) and through the Railroads for National Defense Program,[84] SDDC designates and continuously reviews STRACNET to verify the readiness of this "minimum interconnected system of main rail lines needed for swiftly moving defense equipment and materiel" within the continental United States.[85]

More broadly, the FRA is responsible for the regulatory oversight and safety of all U.S. rail systems, while TSA is charged with ensuring their security from external threats.[86] Rather than evaluating a company's compliance with a standardized checklist

of cybersecurity policies, TSA's performance-based approach judges covered entities on the results of their cybersecurity efforts. For companies that do not meet the performance metrics, TSA has focused on jointly developing action plans rather than using enforcement measures like fines to strengthen a company's cybersecurity posture.[87]

In addition to cyber threats from nation-states and criminals seeking to compromise critical infrastructure, the U.S. rail subsector also faces growing foreign penetration of its supply chain.

TSA issued its first security directives for freight and passenger rail systems in December 2021, requiring covered entities to designate a cybersecurity coordinator, report cybersecurity incidents to CISA, develop cybersecurity incident response plans, and conduct cybersecurity vulnerability assessments.[88] Updated guidance in July 2024 further required these entities to establish and implement TSA-approved cybersecurity implementation plans and develop annually updated cybersecurity assessment plans.[89]

In November 2024, TSA issued a notice of proposed rulemaking that would formalize these security directives while maintaining its performance-based approach.[90] For the most part, the proposed rule would simply mandate the requirements that were previously included in the security directives. The proposed rule also attempts to align with cybersecurity standards from the National Institute of Standards and Technology and with CISA's cross-sector cybersecurity performance goals.[91]

For freight rail, entities subject to the security directives and the proposed rule are limited to Class I railroads; railroads transporting hazardous materials; short-line railroads connecting two or more Class I railroads; and railroads that are part of STRACNET. In total, TSA estimates that 73 of the approximately 620 freight railroads would be subject to the proposed rule.[92]

TSA further acknowledges the costs involved in implementing the requirements to have a cybersecurity risk management program and report incidents to the federal government. Without discounting for existing capabilities that covered freight railroads may already have, TSA estimates that the rule would cost freight rail companies a combined $685 million over 10 years, or a little less than $1 million per year per covered entity.[93]

TSA's efforts to require freight rail operators to improve their cybersecurity have been met with mixed reactions from industry. While the Association of American Railroads (AAR) asserts that its members have long focused on cybersecurity, firms specializing in cybersecurity of industrial control systems warn that the industry has lagged behind other critical infrastructure owners and operators.[94] AAR President Ian Jefferies testified to Congress in November 2024 that TSA has not sought enough industry input.[95] At the same hearing, however, TSA officials noted that they host biweekly calls with rail owners and operators subject to the security directives.[96]

In addition to cyber threats from nation-states and criminals seeking to compromise critical infrastructure, the U.S. rail subsector also faces growing foreign penetration of its supply chain. In recent years, Beijing has aggressively supported the state-owned enterprise China Railway Rolling Stock Corporation (CRRC), which has become the world's largest manufacturer of locomotives and railcars.[97] As strategic intelligence firm Veretus Group observed in 2019, "underpricing and anticompetitive behavior" led CRRC to decimate Australia's freight rail manufacturing and take over the industry.[98] CRRC has also started to make inroads into the U.S. market by securing metro and transit rail contracts in a number of major American cities, such as Boston, Los Angeles, and Chicago.[99]

Concerns about CRRC reached a tipping point when the company was bidding to upgrade the trains on the Washington Metropolitan Area Transportation Authority network in 2019.[100] The contract included provisions for video surveillance systems, monitoring and diagnostics equipment, data interface capabilities with the rail network, and connected train control and safety systems, demonstrating the variety of connected systems included in modern railcars.[101] Senators raised national security concerns,[102] and CRRC lost the bid.[103] Since then, DoD has placed CRRC on the Pentagon's entity list of Chinese military companies operating in the United States, known as the Section 1260H list.[104] Entities on this list are not subject to sanctions or other restrictions outright, but lawmakers intended the list to discourage domestic and foreign companies from doing business with firms supporting China's military capabilities.

Nevertheless, CRRC subsequently won contracts for seven U.S. transit rail projects, worth a total of $4.3 billion.[105] This is not merely a commercial concern. In testimony before the House Committee on Transportation in May 2019, retired U.S. Army

Brig. Gen. John Adams warned, "Chinese penetration of the rail system's cyber-structure would provide early and reliable warning of U.S. military mobilization and logistical preparations for conflict."[106] China's efforts to dominate the U.S. market had been somewhat restricted by local content requirements for railcars used on passenger rail networks. But Adams further warned that Beijing "is banking on the fact that once CRRC secures sufficient U.S. municipal transit contracts, it can pivot quickly and inexpensively toward the more strategically important freight rail sector."[107]

Luckily, however, the U.S. government has grown wise to this scheme. As part of the bipartisan infrastructure law passed in 2021, Congress required the FRA to block China from infiltrating U.S. freight rail. The FRA subsequently proposed banning new freight cars manufactured in countries of concern, garnering praise from industry associations of rail manufacturers and suppliers.[108] The final rule went into effect in January 2025, requiring that no railcars manufactured after December 2025 include components or sensitive technology from countries of concern.[109] The regulation, however, does not remove existing Chinese-built stock, nor does it address aftermarket maintenance.

America's past and future military mobility and economic activity are inextricably linked to railways. Compromise of those networks by malicious cyber actors or adversarial suppliers would, in turn, compromise America's national security and economic productivity.

Securing GPS, a DoD Space Asset

The relationship between U.S. military capabilities and critical infrastructure is not a one-way street. The Pentagon owns and operates the Global Positioning System (GPS) satellite network. While initially created as a military system, it has since become a public good and is thus governed by an interagency committee led jointly by DoD and the DOT.[110] GPS provides positioning, navigation, and timing (PNT) services — that is, precise location and timing information by triangulating signals from multiple satellites. While consumers are most familiar with GPS as a tool for navigation — essential in the transportation sector — many other critical infrastructure sectors also rely on GPS. The financial sector, for example, uses GPS for precision timing for global transactions. The electricity subsector similarly uses GPS timing to synchronize power plants.

Over the past two decades, insufficient investment in modernizing GPS has left it vulnerable to jamming and spoofing.[111] The former involves drowning out GPS signals, while the latter tricks the receiver into calculating false location data. While GPS jamming and spoofing incidents that disrupt navigation are most often associated with conflict zones such as the Russia-Ukraine and Israel-Lebanon wars,[112] an October 2022 incident at the Dallas Fort Worth International Airport caused some flights to go off-course and forced pilots to rely on other navigation systems.[113] Spoofing is reportedly affecting as many as 1,000 flights per day globally, disrupting cockpit navigation and safety systems. While these incidents have been temporary and have not resulted in major safety issues, they are a growing concern for the aviation industry.

The GPS system is vulnerable because the L1 frequency, the foundational signal used by both civilian and military systems, lacks modern encryption and anti-jamming features, making it an easy target for interference by malicious actors and environmental factors. The L2 frequency, used alongside L1, improves GPS accuracy, particularly for military applications, by offering advanced error correction that compensates for atmospheric distortions that can affect L1 signals. The L2 frequency, however, is vulnerable to certain types of interference.

The L5 frequency, specifically designed for safety-of-life applications, offers more accurate and reliable data for precision navigation. It features a larger bandwidth, advanced error correction, and significantly improved resistance to jamming and spoofing.[114] However, only the more advanced GPS IIF and GPS III satellites currently broadcast L5.[115] DoD has been years late in launching these satellites, only recently launching the 18th of 21 planned satellites.[116] Additionally, Raytheon's GPS Next Generation Operational Control System (GPS OCX) is years behind schedule. In the absence of these two programs, most existing receivers are not equipped to use L5.[117]

In a July 2024 memo, the President's National Space-Based PNT Advisory Board — an independent White House advisory board on GPS, comprising a distinguished group of academics, industry experts, and former military leaders — urged DoD to activate L5 as soon as possible.[118] The board did not mince words, warning that the joint civilian-military executive committee that is responsible for coordinating GPS-related matters across agencies is "ineffective and nonresponsive to existing and emerging risks." The board further warned that America's "PNT capabilities have fallen behind those of other" global navigation satellite systems, including China's BeiDou.[119]

The good news is that while 21 GPS satellites are required for aviation flight safety certification, other critical infrastructure can rely on a network with only 18 of 21 satellites in orbit as long as DoD and the DOT certify the existing system for all other uses. This certification can occur once the GPS OCX is complete, hopefully in mid- to late 2025. Once this happens, GPS systems will likely be built and procured leveraging the L5 signal. And rail networks, ports, and elements of the aviation infrastructure — as well as other critical infrastructure — will all benefit greatly.

Policy Recommendations

The maritime, aviation, and rail industries are critical to national security, economic productivity, and public health and safety. While these subsectors have a long history of focusing on safety and security, their cybersecurity and resilience demand greater focus. And even though they are essential to military mobility, DoD has limited engagement with federal civilian efforts to collaborate with owners and operators to improve cybersecurity. These findings demand action by Congress, the executive branch, and the private sector. This report offers recommendations focusing on new federal programs and funding to improve the resilience of transportation critical infrastructure related to military mobility.

For All Transportation Systems:

1. **Congress, the executive branch, and independent federal and state regulators should work together to harmonize cybersecurity regulations.**

   Regulatory harmonization should remain a priority for both Congress and the executive branch so that maritime, aviation, and rail operators — and all critical infrastructure owners and operators — can focus on improving their security and resilience rather than proving their compliance with multiple, redundant regulations. Private industry has warned that duplicative regulations strain already tight cybersecurity budgets. Both Airlines for America and the American Association of Railroads, lobbying and trade associations for their respective industries, have argued for the streamlining of compliance processes and deconflicting duplicative regulations at the federal and state levels.[120]

   During the Biden administration, the Office of the National Cyber Director undertook regulatory harmonization efforts to address these and other concerns by encouraging reciprocity between different regulatory and compliance regimes. In other words, if a company demonstrates to one set of regulators that it complies with cybersecurity requirements, it should not need to demonstrate the same facts again to a second regulatory body. This effort should continue under the Trump administration. Members of Congress from both parties, meanwhile, are also on record supporting legislation and other efforts to harmonize regulations, particularly as it relates to cyber incident reporting requirements.

2. **Congress should authorize and appropriate funding for cybersecurity grant programs across all transportation critical infrastructure subsectors vital to military mobility.**

   The DOT has existing grant programs, such as the National Infrastructure Project Assistance program for large-scale improvements in U.S. transportation infrastructure, and the Department of Homeland Security runs freight rail security and transit security grant programs for physical security upgrades. Existing programs, however, do not provide prioritized funding for cybersecurity upgrades. Congress should authorize the departments to require cybersecurity enhancements be included as part of its existing grant programs that support critical infrastructure project planning and construction by private entities as well as state, local, tribal, and territorial governments. Congress should also create the following subsector-specific cybersecurity grant programs.

   a. For the maritime industry:

      Congress should direct the Coast Guard to create a grant program in conjunction with the DOT's Maritime Administration to provide port authorities with funds to improve cybersecurity. Working with DoD, the grant-making agency should prioritize strategic sealift ports. Among other cybersecurity investments, port operators should use grants to offset the costs of purchasing new ship-to-shore cranes from non-adversarial countries.

b. For the aviation industry:

Congress should provide funds for the establishment of a cybersecurity grant program for airport authorities. In addition to prioritizing commercial hubs, the FAA should also work closely with DoD to prioritize grants for major hubs for CRAF carriers and the designated airports with which DoD has arrangements to support military operations.

c. For the freight rail industry:

Congress should direct TSA to create a cybersecurity grant program for short-line freight railroads to improve their cybersecurity protections. In administering the program, TSA should work with DoD to prioritize grants for smaller railroads that are an essential part of STRACNET, those serving as connectors to Class I freight lines, and all other non-Class I freight railroads covered by TSA's proposed cybersecurity rule. Among other priorities, funding should support the proper implementation of sensors and securing other trackside operational technologies.

3. DoD should review interagency coordination and its own implementation of responsibilities for defense critical infrastructure protection.

a. DoD is best positioned to identify the critical infrastructure most essential for supporting military mobility, but mitigating these threats requires cooperation with the sector risk management agencies that uniquely understand this infrastructure. To ensure effective coordination between DoD and SRMAs, the GAO should conduct a review of interagency coordination efforts to secure defense critical infrastructure in the transportation sector. Such a report should identify gaps in general communication, threat intelligence sharing, and mitigation efforts as well as any overlapping, duplicative efforts.

b. In addition, DoD should review the implementation of its own policies. The Office of the Under Secretary for Defense for Policy should review DoD's implementation of defense critical infrastructure protection responsibilities to determine if they have been properly implemented.[121] The assistant secretary of defense for cyber policy should evaluate mission assurance cybersecurity priorities and determine whether the existing list of critical cyber missions, capabilities, functions, systems, and supporting assets is comprehensive.[122] As part of these assessments, DoD should also update guidance on replacing the DISLA designation and reevaluate the sectors it includes as part of defense infrastructure. This should also result in updated or new directives requiring regular cybersecurity assessments for defense critical infrastructure.

4. DoD should conduct national and local exercises with private-sector partners simulating the mobilization of military forces while critical infrastructure sustains cyberattacks.

The Fiscal Year 2024 National Defense Authorization Act instructed DoD to conduct pilot exercises focused on ensuring that military bases — and the utilities servicing them — can restore power, water, and telecommunications quickly in the event of a significant cyberattack.[123] This is a valuable first step, but it remains unclear if DoD has fulfilled this statutory requirement.

Additionally, the U.S. government should expand this program to focus on ensuring that during a significant cyber or other security incident, transportation infrastructure can continue to operate at a minimum level required for military mobility. Exercises should take place at a local level focused on individual military installations and regional hubs to improve resilience and cooperation. Exercises at the national level should inform federal policymaking around continuity-of-economic functions as well as policies around how the military uses excess commercial capacity in the event that increased tensions reduce commercial trade demands.

5. The White House should revise the GPS governance strategy and accelerate the transition to the GPS III architecture and the less vulnerable L5 frequency while also exploring the feasibility of terrestrial PNT.

In its July 2024 memo, the PNT advisory board urged the White House to review Space Policy Directive 7 to "establish a clear strategy" with "clear roles and responsibilities" for modernizing GPS and improving its resilience. The board also urged the U.S. Space Force to establish a pathway toward the speedy adoption of L5 signals.[124] The White House should adopt the board's recommendations and direct DoD and Space Force to prioritize GPS satellite launches.

At the same time, DoD should also explore alternative PNT solutions to provide greater resilience to these services. DoD should conduct a study on the feasibility of using terrestrial PNT services for military and homeland defense purposes within the continental United States. In partnership with the Federal Communications Commission, the Department of Commerce, and other relevant agencies, the study should also explore the viability of these services for civilian and commercial use.

For Maritime Transportation Systems:

6. **The Government Accountability Office should conduct an audit of U.S. Coast Guard requirements to effectively exercise its SRMA responsibilities.**

   In furtherance of the February 2024 executive order clarifying the Coast Guard's cybersecurity authorities, the GAO should conduct an extensive audit of budget allocations, expenditures, and required resources for the Coast Guard to execute its sector risk management and regulatory responsibilities as well as the risk management responsibilities of its captains of the port. The GAO audit should include an assessment of the Coast Guard's current organization to execute its SRMA responsibilities.

7. **Congress should provide additional appropriations to support cyber initiatives conducted by U.S. Coast Guard captains of the port.**

   Based on the findings of that GAO audit, Congress should appropriate additional funding to ensure that the Coast Guard and its captains of the port have the resources necessary to work with port operators and other owners and operators within the maritime systems subsector to assess, identify, and mitigate cyber threats to U.S. maritime infrastructure.

8. **The U.S. Coast Guard and CISA should provide guidance on trusted vendors for maritime operational technology.**

   The House Homeland Security Committee and House Select Committee on the Chinese Community Party's joint report on Chinese investments in the U.S. maritime industry contains short-, medium-, and long-term recommendations to mitigate concerns regarding ZPMC cranes and to coax the market away from their usage.[125] Many of these recommendations simply call on the federal government to issue guidance and commission studies. Congress should exercise oversight to ensure the federal government takes these actions, requiring the U.S. Coast Guard and CISA to detail (in a classified setting if necessary) the contents of maritime security directives and other guidance provided to industry about trusted operational technology vendors.

For the National Airspace System:

9. **Congress should provide oversight and appropriations to ensure that the FAA and TSA collaboration with the private sector is fully resourced.**

   The 2024 FAA reauthorization bill provided the FAA with exclusive rulemaking authority and created a new civil aviation rulemaking committee to work with aircraft manufacturers, airlines, airports, and other stakeholders to develop cybersecurity standards for the subsector.[126] During a congressional hearing in September 2024, witnesses applauded the committee's creation and also complimented TSA's recent efforts to ensure its cybersecurity directives are threat-based and risk-informed.[127] Given the relative immaturity of these efforts, however, Congress should exercise robust oversight to ensure both the FAA and TSA share information with industry in a timely manner and have the necessary resources and expertise to support the subsector.

10. **The FAA should produce a cybersecurity road map report to be delivered to Congress alongside the FAA NextGen Annual Report.**

    a. The FAA should prioritize technology modernization, cybersecurity, and cyber-physical resilience upgrades of systems critical to air traffic control as key pillars of its NextGen program. To this end, Congress should direct the FAA to provide a road map report on cybersecurity improvements that would be issued as part of the NextGen program. The FAA should provide a detailed action plan on how it would continue to integrate newer technologies with legacy air traffic control systems while prioritizing infrastructure security and continuous operations.

    b. Congress should request that the FAA produce an annual report on cybersecurity improvements in the nation's air traffic control systems to be delivered alongside the FAA's NextGen Annual Report. The FAA should utilize the aviation cybersecurity rulemaking committee as part of the development of its action plan.

For the U.S. Freight Rail Industry:

11. TSA should continue investing in building collaboration and trust with rail operators.

TSA should continue working with the industry on its security directives for freight and passenger rail. While TSA holds biweekly meetings with rail companies[128] and regular classified and unclassified briefings with transportation stakeholders,[129] the trade association AAR still contends that there has been "very limited industry input" on the security directives.[130] This pushback likely reflects the natural tension between regulator and regulated entity, but TSA must redouble its efforts to work with rail stakeholders. Congress should likewise exercise oversight to ensure that TSA is devoting the necessary resources to this subsector.

12. The White House should direct an interagency supply chain risk assessment for the U.S. freight rail industry.

a. The president should task the Department of Commerce, in collaboration with DoD, TSA, and the FRA, with producing a supply chain risk assessment to determine critical components for the rail subsector and the reliance of those components on supply chains originating from the People's Republic of China. If the president does not issue this tasking, Congress should do so. Given the new restrictions on Chinese components in new railcars, the assessment should focus on aftermarket maintenance as well as the prevalence of Chinese-made railcars already on U.S. railroads today. As part of this risk assessment, DoD should produce an annex on the national security risk posed by freight rail cars and components produced by state-owned enterprises from countries of concern.

b. In parallel, the Department of Commerce should assess the domestic and allied manufacturing capabilities to produce all passenger and freight rail components (including replacement parts for older railcars) without inputs from countries of concern. Again, if the executive branch does not undertake this activity on its own, Congress should direct it to do so. If manufacturing is not commercially viable, Commerce should propose subsidies, tax incentives, or other programs to bolster domestic and allied production.

13. DoD should produce an annex on cybersecurity and resiliency alongside its five-year STRACNET assessments.

a. To provide an updated threat landscape for domestic freight rail lines, DoD should conduct an analysis of the cyber resiliency of STRACNET and consistently include a cybersecurity assessment within its five-year assessments. Congress may need to update authorizations to clarify this DoD requirement.

Conclusion

During a conflict, America's adversaries are likely to attack U.S. critical infrastructure in an attempt to constrain Washington's policy options, including its capacity to mobilize the armed forces. Inhibiting the U.S. military's ability to move troops and materiel from "fort to port" takes a significant capability off America's chessboard. Ensuring the resilience of U.S. critical infrastructure must be a top priority for the nation as a whole and for DoD in particular.

Endnotes

1. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 2024. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf)

2. Sam Sabin, "China's Volt Typhoon Poses Critical Cyber Threat," *Axios*, February 7, 2024. (https://www.axios.com/2024/02/07/china-volt-typhoon-critical-cyberattacks)

3. Christopher Wray, "Opening Statement: The CCP Cyber Threat to the American Homeland and National Security," *Hearing before the House Select Committee on the Chinese Communist Party*, January 31, 2024. (https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party); U.S. Cybersecurity and Infrastructure Security Agency, "Malware Analysis Report," May 17, 2024. (https://www.cisa.gov/sites/default/files/2024-05/MAR-10448362.c1.v2.CLEAR_.pdf)

4. Joe Warminsky, "FBI says it recently dismantled a second major China-linked botnet," *The Record*, September 18, 2024. (https://therecord.media/fbi-dismantles-flax-typhoon-china-linked-botnet-wray-aspen); Sarah Krouse, Dustin Volz, Aruna Viswanatha, and Robert McMillan, "U.S. Wiretap Systems Targeted in China-Linked Hack," *The Wall Street Journal*, October 5, 2024. (https://www.wsj.com/tech/cybersecurity/u-s-wiretap-systems-targeted-in-china-linked-hack-327fc63b)

5. U.S. Transportation Security Administration, Notice of Proposed Rulemaking, "Enhancing Surface Cyber Risk Management," 89 Federal Register 88488, November 7, 2024, page 88532. (https://www.govinfo.gov/content/pkg/FR-2024-11-07/pdf/2024-24704.pdf)

6. "Sector Risk Management Agencies," *Cybersecurity and Infrastructure Security Agency*, accessed March 4, 2025. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies)

7. The White House, "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)

8. U.S. Department of Defense Manual, "Defense Critical Infrastructure Program (DCIP) Management: DoD Mission-Based Critical Asset Identification Process (CAIP)," DoD Instruction 3020.45, October 24, 2008. (https://irp.fas.org/doddir/dod/m3020_45_v1.pdf)

9. U.S. Department of Defense, Office of Inspector General, "Audit of Protection of Department of Defense Critical Infrastructure," April 9, 2019. (https://media.defense.gov/2019/Apr/09/2002111257/-1/-1/1/DODIG-2019-071.PDF); U.S. Department of Defense, "Instruction 3020.45: Defense Critical Infrastructure Program (DCIP) Management," June 6, 2017. (https://irp.fas.org/doddir/dod/i3020_45.pdf); U.S. Department of Defense, Mission Assurance Construct, "Instruction 3020.45P: Defense Critical Infrastructure Program (DCIP) Program," February 16, 2017. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/302045p.pdf)

10. U.S. Department of Defense Manual, "Defense Critical Infrastructure Program (DCIP) Management: DoD Mission-Based Critical Asset Identification Process (CAIP)," DoD Instruction 3020.45, October 24, 2008. (https://irp.fas.org/doddir/dod/m3020_45_v1.pdf); "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency, accessed March 11, 2025. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors)

11. U.S. Department of Defense Manual, "Defense Critical Infrastructure Program (DCIP) Management," DoD Instruction 3020.45, October 24, 2008. (https://irp.fas.org/doddir/dod/m3020_45_v1.pdf)

12. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Pub. L. 116-283, 134 Stat. 4768, §9002(c). (https://www.congress.gov/bill/116th-congress/house-bill/6395)

13. The White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience)

14. U.S. Trade Numbers, "U.S. Airports, Seaports and Border Crossings," accessed March 4, 2025. (https://ustradenumbers.com/ports)

15. Jiwon Ma and William Loomis, "Full Steam Ahead: Enhancing Maritime Cybersecurity," *Cybersecurity Solarium Commission*, March 28, 2023. (https://cybersolarium.org/csc-2-0-reports/full-steam-ahead-enhancing-maritime-cybersecurity)

16. The U.S. Navy, Military Sealift Command, "Handbook 2023," March 2023. (https://www.msc.usff.navy.mil/Portals/43/Publications/Handbook/MSCHandbook2023-Final.pdf)

17. U.S. Department of Transportation, Maritime Administration, "Fiscal Year 2024 President's Budget," March 2023. (https://www.transportation.gov/sites/dot.gov/files/2023-03/MARAD_FY_2024_President_Budget_508.pdf)

18. Ann C. Phillips, "Review of Fiscal Year 2025 Maritime Transportation Budget Requests, Pt. 1: Maritime Administration and Federal Maritime Commission," *Testimony before the House Committee on Transportation and Infrastructure Subcommittee on Coast Guard and Maritime Transportation*, April 30, 2024. (https://www.transportation.gov/review-fiscal-year-2025-maritime-transportation-budget-requests-pt-1-maritime-administration-and)

19. For more information on MARAD and its Ready Reserve Force and National Defense Reserve Fleet, see U.S. Department of Transportation, Maritime Administration, "Maritime Administration's Ready Reserve Force," accessed March 4, 2025. (https://www.maritime.dot.gov/national-defense-reserve-fleet/ndrf/maritime-administration%E2%80%99s-ready-reserve-force); U.S. Department of Transportation, Maritime Administration, "National Defense Reserve Fleet (NDRF) Fleet and Services," accessed March 4, 2025. (https://www.maritime.dot.gov/national-defense-reserve-fleet/ndrf-fleet-and-services)

20. Bradley Martin and Roland J. Yardley, "Approaches to Strategic Sealift Readiness," *RAND Corporation*, 2019. (https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3049/RAND_RR3049.pdf); Ann C. Phillips, "Posture and Readiness of the Mobility Enterprise," *Testimony before the House Committee on Armed Services Subcommittee on Readiness and Subcommittee on Seapower and Projection Forces*, March 28, 2024. (https://www.transportation.gov/posture-and-readiness-mobility-enterprise)

21. House Select Committee on the Chinese Communist Party, "Letter to TRANSCOM and MARAD," February 6, 2024. (https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2.6.2024%20-%20Letter%20to%20TRANSCOM%20and%20MARAD.pdf)

22. U.S. Department of Transportation, Maritime Administration, "Maritime Administration's Ready Reserve Force," accessed March 4, 2025. (https://www.maritime.dot.gov/national-defense-reserve-fleet/ndrf/maritime-administration%E2%80%99s-ready-reserve-force)

23. RADM Derek Trinque, "Statement for the Record," *Testimony before the House Homeland Security Committee Subcommittee on Transportation and Maritime Security*, February 29, 2024. (https://www.congress.gov/118/meeting/house/116817/witnesses/HHRG-118-HM07-Wstate-TrinqueD-20240229.pdf)

24. U.S. Department of Transportation, Maritime Administration, "National Port Readiness Network (NPRN)," accessed March 4, 2025. (https://www.maritime.dot.gov/ports/national-port-readiness-network-nprn); Rolando C. Baez, "The Strategic Seaport Program: Ensuring Transportation Readiness," *U.S. Army*, January 10, 2017. (https://www.army.mil/article/180466/the_strategic_seaport_program_ensuring_transportation_readiness)

25. Kirsten Trego, Caroline Beckmann, and Justin Jacobs, "Taking Charge! Critical success factors for a captain of the port," *Proceedings: The Coast Guard Journal of Safety & Security at Sea*, Fall 2018. (https://www.dco.uscg.mil/Portals/9/DCO%20Documents/Proceedings%20Magazine/Archive/2018/Vol75_No2_Fall2018.pdf)

26. John Vann, "Port Cybersecurity: The Insidious Threat to U.S. Maritime Ports," *Testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security*, February 29, 2024. (https://democrats-homeland.house.gov/activities/hearings/port-cybersecurity-the-insidious-threat-to-us-maritime-ports)

27. "The Economic Impact of a Port Closure: Full Report," *National Association of Manufacturers and National Retail Federation*, June 2014. (https://www.nam.org/wp-content/uploads/2019/05/NAM-Port-Closure-Full-Report-2014.pdf)

28. U.S. International Trade Commission, "The Impact of the COVID-19 Pandemic on Freight Transportation Services and U.S. Merchandise Imports," *Shifts in U.S. Merchandise Trade 2020*, November 21, 2021. (https://www.usitc.gov/research_and_analysis/tradeshifts/2020/special_topic.html)

29. Alicia Robinson, "Prolonged port closure could cost billions of dollars across regional supply chain," *Long Beach Business Journal*, April 18, 2023, page 2. (https://img.lbpost.com/wp-content/uploads/sites/8/2023/04/18150539/2023-04-18-Issue-08.pdf)

30. Jiwon Ma and Mark Montgomery, "Removing the Trojan Horse from America's Ports," *C4ISRNET*, March 11, 2024. (https://www.c4isrnet.com/opinion/2024/03/11/removing-the-trojan-horse-from-americas-ports)

31. Executive Order 14093, "Executive Order on Amending Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States," February 21, 2024. (https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/02/21/executive-order-on-amending-regulations-relating-to-the-safeguarding-of-vessels-harbors-ports-and-waterfront-facilities-of-the-united-states)

32. The White House, "Fact Sheet: Biden-Harris Administration Announces Initiative to Bolster Cybersecurity of U.S. Ports," February 21, 2024. (https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/02/21/fact-sheet-biden-harris-administration-announces-initiative-to-bolster-cybersecurity-of-u-s-ports)

33. Wayne Arguin and John Vann, "Port Cybersecurity: The Insidious Threat to U.S. Maritime Ports," *Testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security*, February 29, 2024. (https://www.congress.gov/118/meeting/house/116817/witnesses/HHRG-118-HM07-Wstate-ArguinW-20240229.pdf)

34. Jiwon Ma and Maria Rofiro, "U.S. Coast Guard Issues Landmark Cybersecurity Rule to Protect Maritime Infrastructure," *Foundation for Defense of Democracies*, January 23, 2025. (https://www.fdd.org/analysis/2025/01/23/u-s-coast-guard-issues-landmark-cybersecurity-rule-to-protect-maritime-infrastructure)

35. House Committee on Homeland Security, Press Release, "Chairmen Green, Gallagher Slam DHS's Silence, Demand Answers on Threats Posed by Chinese-Manufactured Cranes at U.S. Ports," May 12, 2023. (https://homeland.house.gov/2023/05/12/chairmen-green-gallagher-slam-dhss-silence-demand-answers-on-threats-posed-by-chinese-manufactured-cranes-at-u-s-ports)

36. U.S. Department of Transportation, Maritime Administration, "Adversarial Technological, Physical, and Cyber Influence," *MSCI Advisory*, February 21, 2024. (https://www.maritime.dot.gov/msci/2024-002-worldwide-foreign-adversarial-technological-physical-and-cyber-influence)

37. U.S. Department of Transportation, Maritime Administration, "Study of Cybersecurity and National Security Threats Potentially Posed by Foreign Manufactured Cranes at United States Ports," June 2024. (https://www.maritime.dot.gov/sites/marad.dot.gov/files/2024-06/MARAD%20Study%20of%20Cybersecurity%20and%20National%20Security%20Threats.pdf)

38. RADM Derek Trinque, "Port Cybersecurity: The Insidious Threat to U.S. Maritime Ports," *Testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security*, February 29, 2024. (https://democrats-homeland.house.gov/activities/hearings/port-cybersecurity-the-insidious-threat-to-us-maritime-ports)

39. Aruna Viswanatha, Gordon Lubold, and Kate O'Keeffe, "Pentagon Sees Giant Cargo Cranes as Possible Chinese Spying Tools," *The Wall Street Journal*, March 5, 2023. (https://www.wsj.com/politics/national-security/pentagon-sees-giant-cargo-cranes-as-possible-chinese-spying-tools-887c4ade)

40. "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," *House Committee on Homeland Security and the Select Committee on the Chinese Communist Party*, September 2024, page 4. (https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf)

41. "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," *House Committee on Homeland Security and the Select Committee on the Chinese Communist Party*, September 2024, page 31. (https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf)

42. Ibid., page 29

43. Ibid., page 27

44. Anna Ribeiro, "US Coast Guard issues MARSEC Directive 105-5 for Chinese-made STS cranes amid rising security concerns," *Industrial Cyber*, November 19, 2024. (https://industrialcyber.co/transport/us-coast-guard-issues-marsec-directive-105-5-for-chinese-made-sts-cranes-amid-rising-security-concerns)

45. Issuance of Maritime Security MARSEC Directive 105-5: Cyber Risk Management Actions for Ship-to-Shore Cranes, U.S. Department of Homeland Security, 89 Federal Register 91413, November 19, 2024. (https://www.federalregister.gov/documents/2024/11/19/2024-26896/issuance-of-maritime-security-marsec-directive-105-5-cyber-risk-management-actions-for-ship-to-shore)

46. U.S. House of Representatives, "Division C—Department of Homeland Security," *Explanatory Statement, Appropriations Act, 2024*, March 18, 2024. (https://docs.house.gov/billsthisweek/20240318/Division%20C%20Homeland.pdf)

47. U.S. Department of Transportation, Federal Aviation Administration, Air Traffic Organization, "Air Traffic by the Numbers, 2024," May 2024. (https://www.faa.gov/air_traffic/by_the_numbers/media/Air_Traffic_by_the_Numbers_2024.pdf)

48. U.S. Department of Transportation, Office of Inspector General, "FAA's Progress in Complying with the FAA Extension, Safety, and Security Act of 2016," July 27, 2017. (https://www.oig.dot.gov/sites/default/files/FAA%20Progress%20in%20Complying%20with%20the%20Extension%20Safety%20and%20Security%20Act%20-%207-27-17.pdf)

49. Adam Janofsky, "Cyber Incident at Boeing Subsidiary Causes Flight Planning Disruptions," *The Record*, November 2, 2022. (https://therecord.media/cyber-incident-at-boeing-subsidiary-causes-flight-planning-disruptions)

50. Tom Krisher and David Koenig, "Explainer: How NOTAM Caused Widespread Flight Disruptions," *Associated Press*, January 11, 2023. (https://apnews.com/article/science-federal-aviation-administration-business-9e277db75130cc7e4d4b6c6a7bdaad7c)

51. John Grant, "CrowdStrike Travel Chaos: Airlines Struggling Back to Normal Operations," *OAG*, July 22, 2024. (https://www.oag.com/blog/crowdstrike-travel-chaos-airlines-struggling-back-to-normal-operations)

52. "Federal Aviation Administration's (FAA's) Troubled NOTAM System Has Been on Congress's Radar for Years," *Congressional Research Service*, January 19, 2023. (https://crsreports.congress.gov/product/pdf/IN/IN12078)

53. U.S. Department of Transportation, Office of Inspector General, "FAA Is Taking Steps to Properly Categorize High-Impact Information Systems but Security Risks Remain Until High Security Controls Are Implemented," August 2, 2021. (https://www.oig.dot.gov/sites/default/files/REDACTED%20Final%20Report%20on%20FAA%20System%20Security%20Re-Categorizations.pdf)

54. James H. Williams and T.L. Signore, "National Airspace System Security Cyber Architecture," *The MITRE Corporation*, 2025. (https://apps.dtic.mil/sti/pdfs/AD1125596.pdf)

55. U.S. Department of Defense, "DoD Directive 5030.19, DoD Responsibilities on Federal Aviation," March 6, 2023, pages 3-4. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/503019p.pdf?ver=kXwPF30cLr5h9yJFNUNwHg%3D%3D)

56. "Air Traffic Control: FAA Actions Are Urgently Needed to Modernize Aging Systems," *Government Accountability Office*, September 23, 2024. (https://www.gao.gov/products/gao-24-107001)

57. Kevin Walsh, "Air Traffic Control: Urgent FAA Actions Are Needed to Modernize Aging Systems," *Testimony before the Senate Committee on Commerce, Science, and Transportation Subcommittee on Aviation Safety, Operations, and Innovation*, December 12, 2024. (https://www.gao.gov/products/gao-25-107917)

58. U.S. Department of Transportation, Office of Inspector General, "FAA Is Taking Steps to Properly Categorize High-Impact Information Systems but Security Risks Remain Until High Security Controls Are Implemented," August 2, 2021. (https://www.oig.dot.gov/sites/default/files/REDACTED%20Final%20Report%20on%20FAA%20System%20Security%20Re-Categorizations.pdf)

59. U.S. Department of Transportation, Office of Inspector General, "FAA Has Made Progress but Additional Actions Remain to Implement Congressionally Mandated Cyber Initiatives," March 20, 2019. (https://www.oig.dot.gov/sites/default/files/FAA%20Cybersecurity%20Program%20Final%20Report%5E03.20.19.pdf)

60. U.S. Department of Transportation, Federal Aviation Administration, "National Plan of Integrated Airport Systems (NPIAS) 2023-2027," September 30, 2022, page 13. (https://www.faa.gov/sites/faa.gov/files/npias-2023-2027-narrative.pdf); FAA's updated 2025-2029 NPIAS does not specify if the number of airports with which DoD has this arrangement has changed. U.S. Department of Transportation, Federal Aviation Administration, "National Plan of Integrated Airport Systems (NPIAS) 2025-2029," September 30, 2024. (https://www.faa.gov/airports/planning_capacity/npias/current)

61. Elise Takahama, "Sea-Tac refuses to pay 100-bitcoin ransom after August cyberattack," *The Seattle Times*, September 18, 2024. (https://www.seattletimes.com/seattle-news/sea-tac-refuses-to-pay-100-bitcoin-ransom-after-august-cyberattack)

62. U.S. Air Force, Air Mobility Command, "Civil Reserve Air Fleet," January 2025. (https://www.amc.af.mil/About-Us/Fact-Sheets/Display/Article/144025/civil-reserve-air-fleet)

63. "Federal Aviation Administration's (FAA's) Troubled NOTAM System Has Been on Congress's Radar for Years," *Congressional Research Service*, January 19, 2023. (https://crsreports.congress.gov/product/pdf/IN/IN12078)

64. U.S. Air Mobility Command, "Civil Reserve Air Fleet," Air Mobility Command Instruction 10-402, November 17, 2011. (https://static.e-publishing.af.mil/production/1/amc/publication/amci10-402/amci10-402.pdf)

65. "Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks," *Government Accountability Office*, October 9, 2020. (https://www.gao.gov/products/gao-21-86)

66. Kelly Jackson Higgins, "Boeing 787 On-Board Network Vulnerable to Remote Hacking, Researcher Says," *Dark Reading*, August 7, 2019. (https://www.darkreading.com/vulnerabilities-threats/boeing-787-on-board-network-vulnerable-to-remote-hacking-researcher-says)

67. Equipment, Systems, and Network Information Security Protection, U.S. Department of Transportation, Federal Aviation Administration, 89 Federal Register 67564, August 21, 2024, pages 67564-67572. (https://www.federalregister.gov/documents/2024/08/21/2024-17916/equipment-systems-and-network-information-security-protection)

68. Ibid.

69. Transportation Security Administration, Press Release, "TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators," March 7, 2023. (https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft)

70. "Aviation Cybersecurity Threats," *Testimony before the Senate Committee on Commerce, Science, and Transportation*, September 18, 2024. (https://www.commerce.senate.gov/2024/9/aviation-cybersecurity-threats)

71. Enhancing Surface Cyber Risk Management, U.S. Department of Homeland Security, Transportation Security Administration, 89 Federal Register 88488, November 7, 2024, pages 88488-88592. (https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management)

72. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 7, 2022. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf); Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 6, 2023. (https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf)

73. Rail Safety Improvement Act of 2008, Pub. L. 110-432, 122 Stat. 4856, §104. (https://railroads.dot.gov/sites/fra.dot.gov/files/fra_net/2189/RSIA_Pub.%20L.%20No.%20110-432%20in%20pdf.pdf); U.S. Department of Transportation, Federal Railroad Administration, "Information Guide on Positive Train Control in 49 CFR Part 236, Subpart I," December 12, 2022. (https://railroads.dot.gov/sites/fra.dot.gov/files/2022-12/2022_12%20PTC%20FAQs_final.pdf)

74. U.S. Department of Transportation, Federal Railroad Administration, "PTC Communications: Cybersecurity Technology Review and Concept of Operations," December 2023. (https://railroads.dot.gov/sites/fra.dot.gov/files/2023-12/PTC%20Comms%20ConOps.pdf)

75. Claudia Swain, "The Emerging Cyber Threat to the American Rail Industry," *Lawfare*, October 20, 2022. (https://www.lawfaremedia.org/article/emerging-cyber-threat-american-rail-industry)

76. Amtrak Office of Inspector General, "Information Technology: Better Identifying and Tracking Operational Technology Assets Across the Company Would Improve Cybersecurity," November 7, 2022. (https://amtrakoig.gov/sites/default/files/reports/OIG-A-2023-002%20IT%20Asset%20Inventory_Redacted.pdf)

77. Tom Farmer and Rick Holmes, "Cybersecurity Considerations Relating to Rail Transportation," *National Petroleum Council*, December 10, 2019. (https://www.energy.gov/sites/default/files/2022-10/Infra_Topic_Paper_4-17_FINAL.pdf)

78. Gregory S. Capra, "Protecting Critical Rail Infrastructure," *U.S. Air Force Counterproliferation Center*, December 2006. (https://media.defense.gov/2019/Apr/11/2002115504/-1/-1/0/38CRITICALRAILINFRASTRUCTURE.PDF)

79. U.S. Department of Transportation, Federal Railroad Administration, "Freight Rail Overview," February 24, 2025. (https://railroads.dot.gov/rail-network-development/freight-rail-overview); U.S. Department of Transportation, Bureau of Transportation Statistics, "2019 Pocket Guide to Transportation," January 2019. (https://www.bts.gov/sites/bts.dot.gov/files/docs/browse-statistical-products-and-data/pocket-guide-transportation/224731/pocket-guide-2019.pdf)

80. "The Impacts of State-Owned Enterprises on Public Transit and Freight Rail Sectors," *Testimony before the House Committee on Transportation and Infrastructure*, May 16, 2019, page 21. (https://www.congress.gov/116/chrg/CHRG-116hhrg37138/CHRG-116hhrg37138.pdf)

81. "Defense Transportation: The Army Should Take Action to Better Ensure Adequate Rail Support to Combatant Commanders," *Government Accountability Office*, August 2021. (https://www.gao.gov/assets/gao-21-411.pdf)

82. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, "DOD Manual 4510.12: DOD Transportation Engineering Program," June 14, 2023. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/451012p.PDF?ver=IUaRk8crrj_7lOkYvIaRYg%3D%3D)

83. "Railroads for National Defense," *Surface Deployment and Distribution Command, Transportation Engineering Agency*, accessed March 4, 2025. (https://www.sddc.army.mil/sites/TEA/Functions/SpecialAssistant/Pages/RailroadsNationalDefense.aspx)

84. Surface Deployment and Distribution Command, Transportation Engineering Agency, "Strategic Rail Corridor Network (STRACNET) and Defense Contractor Lines," 2023 Edition. (https://www.sddc.army.mil/sites/TEA/Functions/SpecialAssistant/RND%20Publications/STRACNET%202023.pdf)

85. U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition and Sustainment, "DOD Manual 4510.12: DOD Transportation Engineering Program," June 14, 2023. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/451012p.PDF?ver=IUaRk8crrj_7lOkYvIaRYg%3D%3D)

86. U.S. Department of Homeland Security, "Appendix A: Aviation Security Plan," June 18, 2023, page 69. (https://www.dhs.gov/sites/default/files/2023-06/NSTS_Appendices_Final_4_18_23_508C.pdf)

87. Discussion among TSA officials and industry representatives, June 2024.

88. U.S. Department of Homeland Security, Transportation Security Administration, "Security Directives and Emergency Amendments," accessed March 4, 2025. (https://www.tsa.gov/sd-and-ea); U.S. Department of Homeland Security, Transportation Security Administration, "Security Directive 1580-21-01: Enhancing Rail Cybersecurity," December 31, 2021. (https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf)

89. U.S. Department of Homeland Security, Transportation Security Administration, "Issuance of Security Directive 1580/82-2022-01C: *Rail Cybersecurity Mitigation Actions and Testing*," July 1, 2024. (https://www.tsa.gov/sites/default/files/tsa-security-directive-1580_82-2022-01c-and-memo-508c.pdf)

90. Transportation Security Administration, Press Release, "TSA Announces Proposed Rule That Would Require the Establishment of Pipeline and Rail Cybersecurity Programs," November 6, 2024. (https://www.tsa.gov/news/press/releases/2024/11/06/tsa-announces-proposed-rule-would-require-establishment-pipeline-and)

91. Enhancing Surface Cyber Risk Management, U.S. Department of Homeland Security, Transportation Security Administration, 89 Federal Register 88488, November 7, 2024. (https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management)

92. 49 CFR § 1580.101, "Applicability," n.d. (https://www.law.cornell.edu/cfr/text/49/1580.101); Enhancing Surface Cyber Risk Management, U.S. Department of Homeland Security, Transportation Security Administration, 89 Federal Register 88488, November 7, 2024. (https://www.federalregister.gov/documents/2024/11/07/2024-24704/enhancing-surface-cyber-risk-management)

93. Catherine Stupp, "TSA Wants to Expand Cyber Rules for Pipelines and Railroads," *The Wall Street Journal*, November 8, 2024. (https://www.wsj.com/articles/tsa-wants-to-expand-cyber-rules-for-pipelines-and-railroads-011b9d96)

94. Eric Geller, "Cyberthreats to railroads loom as industry and TSA grow an uneasy partnership," *The Record*, September 24, 2024. (https://therecord.media/railroad-cyberthreats-tsa-regulations)

95. "Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector," *Testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security*, November 19, 2024. (https://homeland.house.gov/hearing/impacts-of-emergency-authority-cybersecurity-regulations-on-the-transportation-sector)

96. Chad Gorman and Steve Lorincz, "Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector," *Testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security*, November 19, 2024. (https://homeland.house.gov/wp-content/uploads/2024/11/2024-11-19-TMS-HRG-Testimony.pdf)

97. John Adams, "National Security Vulnerabilities of the U.S. Freight Rail Infrastructure and Manufacturing Sector – Threats and Mitigations," *Rail Security Alliance*, October 22, 2018. (https://railsecurity.org/wp-content/uploads/2018/10/RSA-National-Security-Risks-to-US-Freight-Rail-Report-Final.pdf)

98. Veretus Group, "U.S. Freight Rail & Transit Cyber Vulnerabilities," *Rail Security Alliance*, July 16, 2019. (https://railsecurity.org/wp-content/uploads/2019/08/US-Freight-Rail-and-Transit-Cyber-Vulnerabilities-Updated-July-16-2019.pdf)

99. John Adams, "National Security Vulnerabilities of the U.S. Freight Rail Infrastructure and Manufacturing Sector – Threats and Mitigations," *Rail Security Alliance*, October 22, 2018. (https://railsecurity.org/wp-content/uploads/2018/10/RSA-National-Security-Risks-to-US-Freight-Rail-Report-Final.pdf)

100. Letter from U.S. Senators to Paul J. Widefeld, January 18, 2019. (https://s3.documentcloud.org/documents/5690574/WMATA-Cyber-Concerns-8000-Series-Rail-Car-RFP.pdf)

101. Erik Olson, "Securing U.S. Surface Transportation from Cyber Attacks," *Testimony before the House Committee on Homeland Security Subcommittee on Transportation and Maritime Security and Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation*, February 26, 2019. (https://docs.house.gov/meetings/HM/HM07/20190226/108931/HHRG-116-HM07-Wstate-OlsonE-20190226.pdf)

102. Sean Lyngaas, "Senators worry that new D.C. Metro railcars could carry cyber risk," *CyberScoop*, January 21, 2019. (https://cyberscoop.com/dc-metro-wmata-china-cars-cybersecurity-risk)

103. Monique Mansfield, "DC's Metro Parts Ways With CRRC," *Alliance for American Manufacturing*, January 28, 2020. (https://www.americanmanufacturing.org/blog/d-c-s-metro-parts-ways-with-crrc)

104. U.S. Department of Defense, "Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. ("Mac") Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116-283)," October 5, 2022. (https://media.defense.gov/2022/Oct/05/2003091659/-1/-1/0/1260H%20COMPANIES.PDF)

105. Rail Security Alliance, Press Release, "U.S. Defense Department Ties CRRC to Chinese Military – Sanctions Possible," October 11, 2022. (https://railsecurity.org/wp-content/uploads/2022/10/Entity-List-Press-Release.101122.pdf)

106. John Adams, "The Impacts of State-Owned Enterprises on Public Transit and Freight Rail Sectors," *Testimony before the House Committee on Transportation and Infrastructure*, May 16, 2019, page 21. (https://www.congress.gov/116/chrg/CHRG-116hhrg37138/CHRG-116hhrg37138.pdf)

107. Ibid., page 20

108. Joanna Marsh, "FRA's proposed rule on certifying rail car origins earns kudos from trade groups," *Freight Waves*, December 11, 2023. (https://www.freightwaves.com/news/fras-proposed-rule-on-certifying-rail-car-origins-earns-kudos-from-trade-groups)

109. Erik Olson, "SOEs Barred from U.S. Freight Car Market," *Railway Age*, January 8, 2025. (https://www.railwayage.com/mechanical/freight-cars/soes-barred-from-u-s-freight-car-market)

110. Theresa Hitchens, "White House advisory group blasts US government, DoD inattention to GPS woes," *Breaking Defense*, August 14, 2024. (https://breakingdefense.com/2024/08/white-house-advisory-group-blasts-us-government-dod-inattention-to-gps-woes)

111. "Final Report of the GPS Spoofing Workgroup," *OPS GROUP*, September 6, 2024. (https://ops.group/dashboard/wp-content/uploads/2024/09/GPS-Spoofing-Final-Report-OPSGROUP-WG-OG24.pdf)

112. Joseph Gedeon, "Can't teach an old GPS new tricks," *Politico*, May 28, 2024. (https://www.politico.com/newsletters/weekly-cybersecurity/2024/05/28/cant-teach-an-old-gps-new-tricks-00160066)

113. Andrew Tangel and Drew FitzGerald, "Electronic Warfare Spooks Airlines, Pilots, and Air-Safety Officials," *The Wall Street Journal*, September 23, 2024. (https://www.wsj.com/business/airlines/electronic-warfare-spooks-airlines-pilots-and-air-safety-officials-60959bbd)

114. "New Civil Signals," *GPS.gov*, August 10, 2020. (https://www.gps.gov/systems/gps/modernization/civilsignals)

115. Sandra Erwin, "GPS startup bets on advanced signal to counter jamming threats," *SpaceNews*, July 17, 2024. (https://spacenews.com/gps-startup-bets-on-advanced-signal-to-counter-jamming-threats)

116. Sandra Erwin, "Experts raise concerns about U.S. commitment to GPS modernization," *SpaceNews*, December 8, 2023. (https://spacenews.com/experts-raise-concerns-about-u-s-commitment-to-gps-modernization); Weslan Hansen, "Experts Warn U.S. Falling Behind in GPS Race," *MeriTalk*, November 5, 2024. (https://www.meritalk.com/articles/experts-warn-u-s-falling-behind-in-gps-race)

117. Nathan Simington, Robert M. McDowell, Dana Goward, Todd Humphreys, Zak Kassas, Mark Montgomery, and Harold Furchtgott-Roth, "Navigating GPS Vulnerabilities: Implications for U.S. Economic and National Security," *Event Hosted by the Hudson Institute*, November 4, 2024. (https://www.hudson.org/events/navigating-gps-vulnerabilities-implications-us-economic-national-security-robert-mcdowell)

118. Theresa Hitchens, "White House advisory group blasts US government, DoD inattention to GPS woes," *Breaking Defense*, August 14, 2024. (https://breakingdefense.com/2024/08/white-house-advisory-group-blasts-us-government-dod-inattention-to-gps-woes)

119. U.S. National Space-Based Positioning, Navigation, and Timing Advisory Board, "Report of the 30th National Space-based PNT Advisory Board Meeting and Associated Activities," July 19, 2024. (https://www.gps.gov/governance/advisory/recommendations/2024-07-PNTAB-chair-memo.pdf)

120. Office of the National Cyber Director, "Cybersecurity Regulatory Harmonization RFI Summary," June 2024. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/06/Cybersecurity-Regulatory-Harmonization-RFI-Summary-ONCD.pdf)

121. U.S. Department of Defense, DoD Directive 3020.40, "Mission Assurance," September 11, 2018, page 6. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983)

122. U.S. Department of Defense, DoD Directive 3020.40, "Mission Assurance," September 11, 2018, page 7. (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf?ver=2018-09-11-131221-983)

123. National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, 137 Stat. 548, § 1517. (https://www.congress.gov/bill/118th-congress/house-bill/2670/text)

124. "Membership," *GPS.gov*, December 1, 2024. (https://www.gps.gov/governance/advisory/members)

125. "Handling Our Cargo: How the People's Republic of China Invests Strategically in the U.S. Maritime Industry," *House Committee on Homeland Security and the Select Committee on the Chinese Communist Party*, September 2024, pages 9-10. (https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/Joint%20Homeland-China%20Select%20Port%20Security%20Report-compressed.pdf)

126. FAA Reauthorization Act of 2024, Pub. L. 118-63, 138 Stat. 1145, §395. (https://www.congress.gov/bill/118th-congress/house-bill/3935/text)

127. "Aviation Cybersecurity Threats," *Hearing before the Senate Committee on Commerce, Science, and Transportation*, September 18, 2024. (https://www.commerce.senate.gov/2024/9/aviation-cybersecurity-threats)

128. Eric Geller, "Cyberthreats to railroads loom as industry and TSA grow an uneasy partnership," *The Record*, September 24, 2024. (https://therecord.media/railroad-cyberthreats-tsa-regulations)

129. Annie Fixler Interview With TSA officials, March 1, 2024

130. Eric Geller, "Cyberthreats to railroads loom as industry and TSA grow an uneasy partnership," *The Record*, September 24, 2024. (https://therecord.media/railroad-cyberthreats-tsa-regulations)

About the Authors

Annie Fixler is the director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies and an FDD research fellow. She works on issues related to cyber-enabled economic warfare, the national security implications of cyberattacks on economic targets, adversarial strategies and capabilities, and U.S. cyber resilience. She also contributes to the work of FDD's Transformative Cyber Innovation Lab and Center on Economic and Financial Power.

RADM (Ret.) Mark Montgomery is the senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. He also directs CSC 2.0, having served as the Cyberspace Solarium Commission's executive director. Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017.

Rory Lane is a cybersecurity and emerging technologies research specialist with an M.A. in international security from the University of Denver's Josef Korbel School of International Studies, as well as a former FDD intern. With expertise in the intersection of cybersecurity, national security, and intelligence studies, Rory focuses on emerging technological threats and their geopolitical implications and has contributed to policy discourse on advancing strategies for secure domestic critical infrastructure, mitigating U.S. cyber risks, and analysis of technological trends.

ACKNOWLEDGEMENTS

The authors would like to thank the experts from government, the U.S. military, and private industry who provided invaluable insights and feedback during the research and writing process. The paper is stronger for their input, although any errors in fact or judgment are ours alone. We are grateful to John Hardie, David Adesnik, and Tzvi Kahn for their rigorous edits and to Daniel Ackerman for the design and production of this report.

Cover Photo: An FDD design collage featuring from left to right: a U.S. Navy aircraft carrier (pigphoto via Getty Images), an F-16 Fighting Falcon fighter (Harald Tittel/picture alliance via Getty Images), a narrow body aircraft (Thiago B Trevisan via Shutterstock), a shipping port (Travel mania via Shutterstock), and passenger trains (Clare Louise Jackson via Shutterstock)

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

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

Mike J. Gallagher, Former 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

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Chris Inglis, Former National Cyber Director

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

Ben Sasse, Former U.S. Senator for Nebraska

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

Partners

FDD | CCTI | CMPP

CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission