# National Security Vulnerabilities of the U.S. Freight Rail Infrastructure and Manufacturing Sector – *Threats and Mitigation*

**Brigadier General John Adams, US Army (Retired)**

October 22, 2018

October 22, 2018

Our country depends upon the privately owned and operated North American freight railroad system to provide safe, reliable, and effective transportation for our nation's industries, our defense industrial base and to ensure the security of our homeland. Our nation's future depends upon the reliability and security of freight rail as the primary mode of transportation not only for every imaginable type of industrial cargo, but also for military equipment, fuels, chemicals, and hazardous waste. 140,000 miles of main-line U.S. freight rail infrastructure connect ports to rural and urban inland hubs, tie military bases to key logistical nodes throughout the nation, and link the U.S. to key allies and trading partners.

In short, U.S. freight rail is crucial to our nation's global economic competitiveness and a strategic asset that our armed forces depend upon to maintain readiness and preserve our defense capacity.

Yet, while we have recognized certain threats to the security of our freight rail system, we have begun to allow foreign interests to make incursions into the rail industry in ways that could threaten our national interests for decades to come. The Government of China has made it a priority to target the U.S. freight rail system, building inroads into freight rail supply chains and taking aim at rolling stock asset ownership. Beijing's "Made in China 2025" plan aims for comparative advantage in the global advanced rail sector, along with nine other industrial sectors. Now is the time for our nation to push back on China's strategy to overtake U.S. freight rail, because a failure to do so means tremendous security risk at home. As a retired Brigadier General and 30-year veteran of the U.S. Army, I know that Chinese dominance of U.S. rail would turn the system from a bedrock industrial and strategic asset into a potentially crippling vulnerability.

In the pages that follow, I review the many reasons that we should be concerned about the advancing efforts by the Government of China to take control of U.S. freight rail; reflect on the state of those efforts thus far; and make specific recommendations for policy action that should be taken to keep our rail, and our nation, safe.

John Adams
Brigadier General, U.S. Army (Retired)
President, Guardian Six Consulting LLC

# Executive Summary

The privately owned and operated U.S. freight rail system is the most sophisticated, productive, and capital-intensive in the world. Freight rail is vital to our economy, our commercial transportation system, and our homeland security infrastructure. Today, on more than 140,000 miles of track, freight rail carries 40% of all American intercity freight and 13% of the nation's goods.

The sustainability of this extensive and sophisticated network is now under threat as the Government of China seeks to make inroads into increasingly large and vital portions of the freight rail manufacturing sector and its supply chain. Unlike other transportation sectors, freight rail products do not have Buy America protections. Therefore, Chinese state-owned enterprises (SOEs) could undercut U.S. suppliers. If we allow Chinese SOEs to continue their efforts to target and undermine U.S. freight rail interests, we risk not only tens of thousands of U.S. jobs, but also larger potential damage to the industrial base, our critical infrastructure, and the security of this nation.

The threat of Chinese dominance of our freight rail sector is more than just a market concern. The national security implications of U.S. industry and military interests being forced to rely on Chinese government-manufactured railcars are jarringly self-evident: 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. Were the Chinese to gain access to advanced U.S. freight car technology (notably specific rolling stock asset health, waybill commodity information on loaded freight cars, or precise GPS train location) the potential exists for the generation of a false negative (or positive) sensor activation – something particularly worrisome given that freight rail carries most nuclear waste and hazardous material that we transport in this nation. A false sensor reading (e.g. tank car outlet dome cover is secure) could lead to a false level of confidence that tank car service valves are secure. If service valves are disturbed and undetected a release of toxic chemicals could result in catastrophic consequences to life and the environment. Moreover, Chinese intelligence about U.S. rail freight logistical movements could provide China with a destabilizing economic competitive edge. Chinese access to or control of U.S. freight rail would also mean that risk of other actors' – including terrorists' – malicious intrusion would become more difficult for U.S operators to detect or counter.

We depend on technology, machinery, and a robust system of intellectual property protections to support our national security; when we allow foreign states to interfere – especially our strategic competitors – we risk that security. While Congress has recognized and taken steps to address similar threats to products such as computer chips and cellular technology, policymakers may not fully understand China's ongoing incursion into an increasingly digitized rail network. Indeed, there are few places where this risk is more acute than with the U.S. freight rail system, and few actors who threaten the security of the freight rail system more than the Chinese government.

Yet in recent years, we have witnessed an unabated and aggressive entry into the U.S. rail market by China's national rail company, China Railway Rolling Stock Corporation (CRRC). This show of force, intended to serve the long-term strategic and technological aims of the Chinese government, as well as that nation's desire to ensure a massive external market for the oversupply of its railcars, components, and raw materials, threatens the survival of U.S. freight rail manufacturing. This, in turn, raises one of the most serious security risks we have faced in the postwar era.

CRRC's history of using underhanded tactics to overtake rail manufacturing in other countries is well known. Over a span of just nine years, CRRC decimated the Australian freight manufacturing marketplace. Now, without immediate action, the U.S. freight rail manufacturing risks a similar fate. If this pattern continues in the U.S., Chinese state-directed efforts will eventually force U.S. companies out of business, endangering as many as 65,000 U.S. manufacturing jobs[1] and putting our national security at risk.

Chinese intrusion into the U.S. rail system's supply chain threatens the health and sustainability of this vital economic pillar, especially in a national emergency. Were China to gain inroads into those operations, management, and supply chains, the ability of U.S. to effectively utilize and leverage the freight rail

network in a crisis could be crippled. Moreover, the extensive telematics and digitization of the American rail network, while integrating the most modern technology, also exposes the system and those who use it to a wide array of cyber risks. While there is no single solution that will mitigate these concerns, we must modernize our national policies to reflect these security risks. Three key reforms are needed from Congress and the administration:

1) Develop comprehensive restrictions and additional reviews on investments from foreign state-backed entities in critical infrastructure integral to our national defense.

2) Ensure that appropriate federal agencies, in coordination with states and localities, develop robust standards for cyber and data integrity applicable to any rail or transit sector contracts involving foreign state-backed entities.

3) Strengthen oversight of Buy America laws to ensure that existing laws and regulations are adhered to in federally-funded transit and rail procurements including railcar manufacturing and explore new avenues to further protect the manufacturing capabilities of freight rail and other core domestic industries that are integral to support and maintain our defense industrial base.

# I. The Impact and Importance of Rail in America

The U.S. freight rail network, in comparison with freight moved by water, pipeline, truck, and air, accounts for approximately 40% of U.S. freight moved by ton-miles and 16% of freight moved as measured by tons.[2] In 2014, the operations and capital expense of the major U.S. freight railroads supported approximately 1.5 million jobs (1.1% of all U.S. workers), nearly $274 billion in U.S. economic output (1.6% of the total), and $88 billion in wages (1.3% of the total).[3] The thoroughly integrated rail systems of the United States, Canada and Mexico are a cornerstone of the North American market as well as the foundation for the safe, reliable, and efficient transportation of goods from rural communities to urban areas to seaports and government and military installations.

Railroads not only serve as the primary mode of transport for an array of key products and commodities, but they also regularly transport U.S. military equipment, hazardous waste, potentially toxic and hazard commodities (i.e. chlorine, anhydrous ammonia, ethylene oxide) and flammable liquids (i.e., petroleum products, ethanol). The North American railcar fleet includes more than 1.6 million cars. With seven Class I railroads,[4] 21 regional railroads, and 525 local railroads,[5] more than 140,000 miles of active railroad, more than 1.65 million freight cars in North America, and 39,521 locomotives, an estimated 12,000 trains operate daily.[6]

The U.S freight rail industry moves more freight than any other rail system worldwide. These figures include the $6.5 billion U.S. freight rail manufacturing sector which directly supports 65,000 jobs.[7] The rail industry provides numerous public benefits including reductions in road congestion, highway fatalities, fuel consumption, logistics costs, and public infrastructure maintenance costs. As private organizations responsible to their shareholders, U.S. freight railroads depend upon profits for reinvestment and capital improvement. The average U.S. manufacturer spends about 3% of revenue on capital expense. The comparable figure for freight railroads is nearly 19%, more than 6 times higher than other industries.[8] The majority of this goes to maintenance and repair, and up to 20% gets reinvested to enhance capacity.[9]

Most commercial freight (i.e. container freight) ships intermodally. Rail's ability to transfer cargo intermodally – train transport of goods before or after transfers from other modes of traffic (aircraft, vessels, or trucks) – is vital to the economic viability of U.S. ports and urban hubs, and for the past four decades, constitutes the fastest growing segment of the freight rail industry.[10] Though the viability of American ports also depends upon the ability to deliver to and receive inland cargo by all transportation modes, freight rail connectivity at ports is increasingly and uniquely important to attract containerized cargo when the origin-destination pairs are more than 500 miles apart. [11] Indeed, U.S. railroads moved over 1 million intermodal loads in July 2018, a 5.5% increase over July 2017.

U.S. military vehicles are transported by freight rail near Greenville, SC in July 2018.

Half of all freight traffic is interchanged. This means that, except for captive unit train movements on a single railroad from origin to destination, using only that railroad's own cars (i.e. coal or grain hoppers), most of the cars in any given freight train will be owned by someone other than the handling carrier. Approximately 70% of all freight cars in North America are owned by non-railroad entities (e.g., private car owners, leasing companies, banks, shippers, and utilities). Interchanged traffic is vital to smooth international commerce for Canada, Mexico, and the United States.

The U.S. freight rail system is also one of the most technologically advanced in the world, with a rapidly expanding scope of digitization, thoroughly incorporating the network into the Internet of Things (IoT). Onboard freight

telematics incorporate a vast network of wireless sensors that monitor asset health and location, sending the information to communication management units as well as to displays in locomotive cabs. U.S. railroads depend upon the continual upgrade and development of advanced technology to reduce risks, improve safety, and improve the network's efficiency. As Federal Railroad Administration (FRA) Administrator Ronald Batory stated at his swearing in on February 28, 2018: "We must aggressively embrace the Internet of Things and artificial intelligence, along with seeking autonomous functions that can foster an environment towards minimal to non-existent risk."[12]

## II. China's Government Aims to Dominate U.S. Rail

Rail manufacturing is one of the 10 industries included in the Chinese government's "Made in China 2025" initiative[13], a plan targeting global dominance in sectors that the Government of China considers most strategic to its global aims. As the White House Office of Trade and Manufacturing Policy noted in a recent report, "[T]he Chinese government has institutionalized the industrial policy of inducing investment in 'encouraged' high technology sectors using the financial resources and regulatory instruments of the State."[14] Toward these ends, China's government has brought to bear a range of state subsidies, state financing, and other resources to support the market entry and market ascension objectives of its wholly government-owned, $33 billion conglomerate, China Railway and Rolling Stock Corporation (CRRC), an enterprise that – with more than 183,000 workers – is now the largest rolling stock producer in the world.[15] While it is owned by the Chinese government, CRRC is *controlled* by the Communist Party of China, and it has set about to build a foothold in the U.S. market, with a near-term goal of overtaking our rail sector.

Indeed, CRRC's own bylaws state that the company will seek guidance from the Communist Party of China on significant matters affecting the company's operations.[16] Three of CRRC's current board members previously held high-level positions at state-owned defense companies, Aviation Industry Corporation of China (AVIC), which produces fighter and bomber aircraft, helicopters, and unmanned aerial vehicles for the Chinese Army, and China Shipbuilding Industry Corporation (CSIC), which produces submarines, warships, and other naval equipment for the Chinese Navy. Furthermore, two former CRRC board members held positions at AVIC and China North Industries Group Corporation Limited (NORINCO), a state-owned defense company that supplies tanks, aircraft, missiles, firearms, and related products for the Chinese military.

The latter two of these entities, CSIC and NORINCO, have been subject to allegations of espionage and sanctions evasion by the U.S. government, raising serious questions about the connections of CRRC board members to these activities. In 2007, AVIC was reputed to have stolen data on the F-35 fighter jet from Lockheed Martin and used it to build the Chinese J-31 fighter.[17] Similarly, CSIC was indicted in 2016 by the U.S. Department of Justice for entering into contracts with another Chinese company for the purchase of industrial materials that were created using stolen trade secrets from an American firm.[18] NORINCO has also been sanctioned by the U.S. State Department on six occasions for contributing to Iranian nuclear weapons development.[19] Two of CRRC's board members were respectively employed in high-level positions at CSIC and NORINCO at the time these offenses occurred, suggesting that they were likely aware of, if not complicit in, this illicit activity.

These actions are a compelling example of how the Communist Party places pressure on SOEs to fulfill directives such as Made in China 2025. To advance these plans, CRRC has first set its sights on the U.S. municipal transit sector, seeking to get major new contracts to sell transit cars to transit agencies in Boston, Chicago, New York, Los Angeles and Philadelphia, among others. The Chinese government 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. There, China can unload much of its current freight car manufacturing capacity oversupply – offsetting its own, slowing domestic market while continuing its strategy of using exports to sustain the nation's employment base.

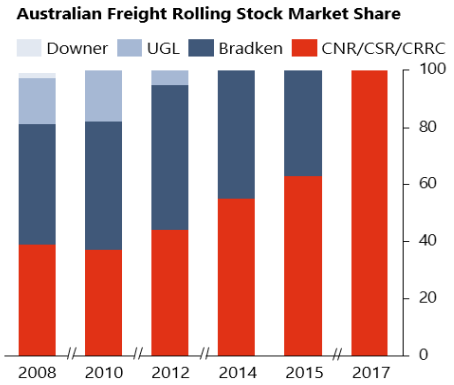
Given China's manufacturing capacity oversupply and long-term goals for global dominance, CRRC hardly needs to profit on short-term sales. As such, the Government of China is able to sweeten CRRC's bids for new U.S. transit

car contracts; not only by subsidizing CRRC's operating costs but also, in many instances, providing below-market financing terms to municipal buyers, making CRRC's prices enticingly low compared to other bids. In fact, CRRC's own 2016 annual report shows that it has leveraged China's state-owned banks to the tune of almost $27 billion to finance its expansion plans.[20] CRRC has used those resources to make its bids for major U.S. project opportunities more attractive, underbidding other competitors by as much as 50%, and — since 2015 – winning $2.6 billion in transit rail contracts to supply "Made in China" railcars for the Boston, Los Angeles, Philadelphia, and Chicago metro systems, among others.[21] Soon, CRRC will have the chance to apply the same tactics to metro transit rail contracts in Atlanta, Washington, D.C., New Jersey and New York City.

With these massive successes under its belt, CRRC has built two U.S. transit assembly plants in Springfield, Massachusetts and Chicago. These are not where railcar manufacturing occurs, since China has little interest in shifting its manufacturing to the United States. Instead, these facilities are where Chinese components and subcomponents are shipped and assembled into cars that are then sold to U.S. buyers. Most of the transit cars must have more than 65 percent of their content sourced from American components if transit authorities want to qualify for federal funding. In the case of the Boston transit contract, however, CRRC met the desire of Massachusetts for an in-state assembly facility and bid the lowest price by more than $150 million under the next competitor.[22] With no federal funding supporting this procurement by the state transit authority MBTA, CRRC avoided all otherwise applicable Federal Transit Administration "Buy America" requirements. In November of last year, CRRC shipped the first fully-built, shrink-wrapped transit rail cars that had been made completely in China into the Port of Boston.

And while U.S. transit rail is typically subject to such domestic content requirements, no similar requirements apply to freight railcar manufacturing. This means that CRRC can effectively import complete or nearly complete freight rail cars to the United States or complete minor assembly at CRRC U.S. facilities at an even lower discount than transit cars have received. Having already established major operations in the U.S., CRRC's current assembly facilities in the United States can easily be modified to accommodate freight assembly as well, which are in fact a downgrade for facilities to produce compared to transit.

CRRC's entry into the freight rail manufacturing poses a direct threat to a major strategic and economic asset of the United States. Indeed, a 2017 Oxford Economics study found Chinese competition in freight rail threatens U.S. economic competitiveness.[23] That same study projected that up to 65,000 U.S. jobs could be eliminated if we allow China to displace U.S. freight rail manufacturing, a sector that has many U.S.-headquartered players today, as well as a long U.S. supply chain since the industry is a major consumer of U.S.-made steel. Even so, signs of Chinese targeting of North American freight rail are already evident, with CRRC having recently opened freight car assembly facilities in Wilmington, North Carolina and Moncton, New Brunswick.[24, 25]



*Source: Oxford Economics*

If the prospect of losing domestic freight rail capabilities seems far-fetched, we need only remind ourselves of recent CRRC activities in Australia to understand how far China is willing to go to dominate in rail. Within a decade after entering Australia's once-thriving domestic rail manufacturing industry, CRRC used underpricing and other anti-competitive tactics as described above to wipe out Australia's domestic rail manufacturing base entirely.[26] Today, Australia's railcar manufacturing is wholly controlled by CRRC. As a clear reminder of China's intentions of continuing ---this trend, CRRC itself Tweeted recently about its plans for market dominance, announcing, "So far, 83% of all rail products in the world are operated by #CRRC or are CRRC ones. How long will it take for us conquering the remaining 17%?"[27]

The European Union and Israel recognize this threat and are exploring and enacting policies to better protect their domestic rail manufacturing and production sectors.[28] [29] As of this writing, even though freight rail is considered by the Department of Homeland Security to be a key element of our nation's critical infrastructure, similar U.S. measures have not been enacted at the federal level to directly protect American freight rail manufacturing from the Government of China and its designs for global dominance.

## III. China's Rail Agenda Threatens U.S. Cybersecurity

***"The possibility of causing mayhem remotely could make train hacking an attractive priority for terrorists."[30]***

In 2010, the world witnessed the first case of weaponized malware when the nuclear industry fell prey to Stuxnet, prompting the possibility of attacks on industrial controls in cyber-systems. The possibility has since become far more real as we have witnessed growing numbers of cyberattacks that threaten and at times undermine key segments of the world's economies, power, financial systems, and other assets.

Predatory Chinese efforts to penetrate our freight rail market create the potential for disruption to the most advanced technologies upon which our rail system depends for safety and efficiency. Commercial railroads are, of course, aware of the risks they face from potential cyber-security incursions and are investing in cybersecurity capabilities. Even so, we significantly increase the risk of Chinese cyber-espionage or even cyber-terrorism by allowing CRRC to displace U.S. rail interests and shift our freight rail supply reliance to the Government of China. If allowed to penetrate the U.S. freight rail system, Chinese government-backed entities could simply vacuum data from individuals and firms connected to the rail network. China's history of cyberattacks on U.S. interests, combined with the Chinese Government's known efforts to use facial recognition and artificial intelligence for tracking its own citizens through "a vast and unprecedented national surveillance system" make this security risk all the more acute.[31]

In other U.S. economic sectors where Chinese SOEs have engaged aggressively, the U.S. Government has responded with targeted restrictions to mitigate clear security risks. Such measures have included a reported U.S. government ban on contracting with the Chinese computer firm Lenovo,[32] a ban on the purchase of Chinese drones,[33] and the removal of Chinese-made security cameras from U.S. military bases.[34] In April 2018, DoD banned Huawei and ZTE cell phones from sale in U.S. military exchanges world-wide.[35] We have yet to do the same to protect Chinese incursions into the U.S. freight rail manufacturing base.

According to the National Institute of Standards and Technology, the following are cyber-threats to industrial control systems, all of which must be taken into account when we consider control of U.S. freight rail assets:

- *Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.*
- *Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.*
- *Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.*
- *ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.*
- *Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.*
- *Interference with the operation of safety systems, which could endanger human life.*[36]

Furthermore, as freight trains become increasingly sophisticated, incorporating more technology and systems integration, these types of cyber-security concerns become more palpable. In U.S. freight rail, industrial controls have replaced the mainframes and protocols that have historically undergirded the industry, and these controls present vulnerabilities not only relative to the freight rail systems themselves, but also through outside data connections that

could threaten both public safety and operating continuity.[37] Significant technology and rapidly expanding IoT capabilities in the U.S. freight rail network create potential security challenges that include:

- **A digitized railroad network/the Internet of Things**: Like other high-tech industries, the freight railroad industry has embraced digitization and the IoT. Integrated teams of data scientists, software developers, and engineers develop and apply technology across every aspect of the nationwide freight rail network. Indeed, such technology has generated significant improvements in operational safety and network efficiency. These benefits also have increased the vulnerability of onboard systems, individual train operations, and perhaps even the industry's metadata warehousing centers to cyber threats.

- **Rail Signaling**: In California in 2008, a Metrolink passenger train collided with a Union Pacific train, causing 25 fatalities and 135 passenger injuries. Congress responded mandating the installation of positive train control (PTC) systems on much of the nation's rail system including the Class I network by 2015. The statutory deadline was later extended by Congress to December 31, 2018, subject to certain alternative schedule criteria. PTC is designed to prevent four specific accident scenarios: train-to-train collisions, over-speed derailments, unauthorized train incursions into right-of-way work zones, and misaligned track switches. A malicious cyber breach of PTC or underlying existing rail signaling systems could wreak havoc and cause accidents on the highly interdependent freight railway network.

- **Locomotives:** Latest generation diesel locomotives have hundreds of sensors which generate thousands of asset health and performance indicators per minute.

- **Onboard Freight Car Location & Asset Health Monitoring**: There are 25,000 freight cars equipped with telematics or remote monitoring equipment. Over 85% of the installations are on tank cars and the vast majority of those are cars carrying hazardous materials: chlorine, anhydrous ammonia, ethylene oxide, and flammable liquids. The tracking technology includes a wireless communication management unit to track precise near-real time lat-long location via GPS, direction of travel, speed, and dwell time within the 45 Transportation Security Administration (TSA) designated high-threat urban areas (HTUAs)[1] and thousands of chemical shipper/consignee defined geo-fences. Wireless sensor nodes measure and/or alert:
  - loaded or empty car condition
  - accelerations and peak impacts in yards & on line-of-road roller bearing temperature
  - lading temperature in tank cars
  - tank car hatch covers open (based upon degree of tilt)
  - handbrake on or off (unattended train securement issue)

- **End-of-Train Telemetry (EOT):** The FRA requires all freight trains operating on excess of 30 mph to be equipped with a 2-way EOT device. EOTs include a flashing blue light indicating the last car in a train as well as the rear brake pipe pressure which is transmitted to the lead locomotive in the train. EOTs also include GPS location. The 2-way feature means that the locomotive engineer can initiate an emergency brake application from the rear of the train as well as the front. This is critical safety technology (a pool of 12,000 devices on the Class I railroads) since Class I railroads are stretching some trains from 10,000 – 12,000 feet long as opposed to a typical 5,000 – 6,000-foot train.

### *A. Industrial Cybersecurity Considerations*

***"Chinese industrial espionage is not new … but it is practiced more openly these days," writes former Navy Secretary J. William Middendorf and the State Department's Dan Negrea.[38] "***

Every company shipping goods on U.S. freight rail – which transports nearly 13% of products across our country, for industries ranging from agriculture to chemicals to mining – should be concerned by the prospect of China controlling key aspects of the U.S. freight rail system. In 2016, U.S. railroads originated over 1.5 trillion tons of freight in 27 million carloads. 40% of all intercity

[1] The Transportation Security Administration defines an HTUA as an area comprising one or more cities and the surrounding areas, including a 10-mile buffer zone.

freight goes by rail, including 67% of the coal used by electric utilities for power generation.[39] Similarly, the chemicals we use to keep our water supply pure and much of the food products we consume are shipped by private freight rail. Therefore, ensuring that these products arrive at their destinations and are free from tampering is of paramount concern.

The Transportation Security Administration, in the Preamble to its November 26, 2008 Rail Transportation Security Final Rule, noted that "Due to the open infrastructure of the rail transportation system, freight trains can be particularly vulnerable to attack" and "[f]reight trains, transporting hazardous materials are of even more concern, because an attack on those trains…could result in the release of hazardous materials" and that "the release of PIH materials in a densely populated urban area would have catastrophic consequences." Rail also carries some of the most hazardous materials (HAZMAT) between industries and military installations in America, often through densely populated areas and cities. Typically railroads move 1.7–1.8 million carloads of HAZMAT every year – items that are essential to our economy and our society – and about 105,000 carloads are so-called "poisonous by inhalation hazard" (TIH) materials such as chlorine or anhydrous ammonia. Freight rail is also a principal mode of transport for nuclear waste. Indeed, the majority of TIH materials in this country are transported via rail, which underscores the paramount emphasis on freight rail safety, free from tampering and malicious intrusion. The safety consequences of any HAZMAT incident, especially those involving the most dangerous worst commodities (e.g. poisonous by inhalation hazard) are substantial: In January 2005, for example, a rail tank car ruptured in Graniteville, SC as the result of a derailment, releasing chlorine that forced the evacuation of 5,400 people within a mile radius of the site. Ultimately 9 people died, and 75 others required treatment for chlorine exposure.[40]

### *B. Transportation Operations Cybersecurity Considerations*

Given the crucial role of rail in our economy and our defense industrial base, U.S. Presidential Policy Directive 21 classifies freight rail as part of our nation's critical infrastructure.[41] And yet, no federal law specifically restricts foreign government ownership of our freight rail supply sector. At the same time, many of the same critical infrastructure features designed to boost the quality of and operation of our freight rail system also raise serious vulnerability concerns in the hands of a foreign government.

Policymakers should recall that the ubiquitous freight rail network traverses nearly every major city in the nation, particularly the 45 TSA designated continental HTUAs. Many rail yards and storage locations are close to densely populated areas, which at any time could contain large numbers of loaded HAZMAT tank cars.[42] Additionally, freight and passenger rail are highly interdependent; they use many of the same bridges, tunnels, control centers, tracks, signals, and switches. Amtrak – the principal U.S. provider of inter-city passenger rail – operates on more than 22,000 miles of track owned by freight railroads, and many commuter and light rail systems also operate on freight rail tracks.[43] A freight rail or railyard incident could be triggered to cause tremendous direct and collateral damage on large population centers as well as vital transportation networks.

Finally, railroads have information-based operating systems that also pose vulnerabilities. The Railway Alert Network (RAN), for instance, distributes intelligence between and among the Federal Rail Administration, commercial railroads and U.S. law enforcement; RAN, which is now operated by the American Association of Railroads (AAR), allows for analysis and dissemination of threat communications from DOT and DHS to AAR's members.[44] Tapping into the RAN system would give an unfriendly outside government access to secure information, including network data analytics and traffic analysis, that should not be shared. The AAR developed its AskRail mobile app in 2014. First responders are able to instantaneously access the specific hazardous materials commodity in a tank car as well as the hazards posed. AskRail employs GIS mapping to identify vulnerable areas like hospitals and schools and rivers. Obviously, unauthorized access to AskRail by those with malicious intent poses a security threat.

### *C. Military Cybersecurity Considerations*

The Department of Defense (DoD) has a longstanding reliance on freight rail in the United States. Most of the military's heavy and tracked vehicles are transported by freight rail meaning that freight rail runs through every military base in the United States.[45] DoD's Military Traffic Management Command (MTMC) has designated nearly 39,000 miles of freight rail track as being

uniquely important to our nation's defense, and thus part of the Strategic Rail Corridor Network, or "STRACNET." STRACNET serves 193 U.S. defense installations, connecting military bases with maritime ports of embarkation and other key points across the country.[46]

Freight rail is also at the heart of the U.S. Transportation Command (TRANSCOM), DoD's global defense transportation system, coordinating people and transportation assets around the world. The Surface Deployment and Distribution Command (SDDC), which is a component of TRANSCOM, operates 10,000 containers and some 1,350 rail cars of its own to deliver equipment and supplies for deployed members of the Army, Navy, Air Force, Marines, and Coast Guard. SDCC also, of course, leverages commercial freight rail to provide important components of DoD's surface transportation requirements.[47] SDCC also utilizes a special heavy-duty flatcar fleet of 1,850 specially designed heavy-duty flatcars managed by a company owned by the major freight railroads.

Because of the deep reliance of our military on U.S. commercial rail, MTMC monitors and evaluates data on railroad industry construction, industry mergers, bankruptcies and other similar events to determine how they may affect DoD's mobility and readiness capabilities. We can assume that MTMC is aware of the ongoing efforts by China's Government to dominate the U.S. rail sector. We must act on this concern to stop CRRC's activities to assert itself in the U.S. marketplace.

## IV. Policy Action is Needed

America's domestic freight rail manufacuring base has always played a vital role in the economic and national security of the United States. As this report demonstrates, freight rail is the lifeblood of the American economy – employing tens of thousands of workers, shipping millions of tons of consumer goods and materials through every major artery in the country and adding over $6.5 billion in GDP. Simultaneously, freight rail is an indispensable part of our nation's defense infrastructure, a vital transportation system that supplies and connects U.S. military installations across the continent. Despite our longstanding reliance on freight rail, America remains unprepared to protect itself from foreign entities with ambitions directly at odds with our own. Even current cooperative efforts between industry and the Department of Homeland Security – while commendable – remain inadequate. The good news is that there is still time to address this threat. Federal and state policymakers have an opportunity to adopt meaningful laws and regulations that can significantly slow the Chinese government's intrusion into the U.S. freight manufacturing space and, in turn, bolster America's security in the face of ever-changing global threats. The goal of this report is to encourage America's political leaders to strongly consider any and all of the following recommendations.

### 1) Develop comprehensive restrictions and reviews on investments from foreign state-backed entities in critical infrastructure integral to our national defense.

The recent reforms to the Committee on Foreign Investment in the United States (CFIUS) through the broadly supported Foreign Investment Risk Review Modernization Act (FIRRMA) were a welcomed step forward for U.S. policy and come at a pivotal moment. Nevertheless, CFIUS continues to face shortcomings. Greenfield investments—wherein a foreign entity creates entirely new investments, rather than through an acquisition, merger, or joint venture—are still not explicitly covered under CFIUS's scope of authority. This means that CRRC and other Chinese SOEs can continue to build new facilities in the U.S. without oversight. To date, only five transactions have ever been blocked by CFIUS,[48] suggesting that we should explore alternative tools to ensure the integrity of the rail manufacturing sector and its associated supply base.

One such tool that has been proposed has been to create a parallel committee to CFIUS under the authority of the Department of Commerce to review transactions for the effects they would have on economic security. With a broader mandate that would allow the Committee to take economic considerations into effect, we could address many of the restrictions that have plagued CFIUS. Another more attainable option is for Congress to take steps to ensure that federal funds are not used to further the aims of SOEs like CRRC. Three of the four manufacturing contracts that CRRC won in the U.S. were awarded using Federal Transit Administration (FTA) dollars, meaning that the U.S. government effectively subsidized a Chinese state-owned enterprise to further the Made in China 2025 initiative at the expense of American workers and security.

**2) Ensure that appropriate federal agencies, in coordination with states and localities, develop robust standards for cyber and data integrity applicable to any rail or transit sector contracts involving foreign state-backed entities.**

As technology continues to advance, so must our standards for cybersecurity. If foreign SOEs are permitted to produce any aspect of the thousands of detector and monitoring systems onboard trains around the country, we will face a continued national security threat capable of halting our entire rail network. These technologies present countless opportunities for hacking and surveillance, and with the cybersecurity risks of other Chinese entities having been well-documented in numerous other industries, action is urgently needed. The Department of Homeland Security and the Department of Transportation should coordinate with state and local agencies to develop and implement standards that ensure cyber and data security for our rail system in any interface with a foreign SOE. These agencies should also engage with private industry to determine what other appropriate measures to address the cybersecurity concerns posed by foreign SOEs and, if appropriate, establish a task force of key stakeholders involved in the manufacturing, operations, and oversight of the freight rail sector. Under new and existing authority, officials must take robust steps to ensure the cyber integrity from any SOE threat of all rail network systems and data streams.

**3) Strengthen oversight of Buy America laws to ensure that existing laws and regulations are adhered to in federally funded transit and rail procurements including railcar manufacturing and explore new avenues to further ensure the manufacturing capabilities of freight rail and other core domestic industries that are integral to support and maintain our defense industrial base.**

CRRC's pattern of investment in other markets like Australia suggest that China will use the transit railcar manufacturing sector as a beachhead to then move into freight railcar manufacturing, implicating even more pressing national security concerns. In the transit railcar manufacturing sector, Buy America laws offer the most comprehensive protections for the industry that, when followed, can help mitigate the financial and strategic advantages that the Government of China offers state-owned companies like CRRC. However, various loopholes and lax enforcement has limited the effectiveness of these laws, allowing CRRC to advance into the transit railcar manufacturing sector unabated.

In April 2017, President Trump signed an executive order to strengthen Buy America laws, requiring federal agencies to develop policies to maximize the use of domestic workers and materials in procurements as well as to recommend new policies to strengthen the implementation of Buy American laws.[49] Nevertheless, little has been done since then to strengthen Buy America. Buy America laws have proven to be a vital protection for the U.S. manufacturing and industrial base, ensuring the employment of thousands of American workers while strengthening our ability to respond to foreign threats in the process. These laws, however, can be easily manipulated as federal agencies often lack the resources to effectively police them, relying all too heavily on the claims of manufacturers and suppliers. When those manufacturers are foreign state-owned enterprises, we have little incentive to take them at their word. Congress and the administration should explore avenues to strengthen domestic content provisions and ensure that existing laws are being followed to protect American workers and security.

## V. Conclusion

The Government of China's attack on our rail system is insidious and ingenious. China enters at the local level, subsidizes the assembly of Chinese transit rail cars, and supplies them to cash-strapped transit systems at bargain prices. In the process, Chinese companies bring small numbers of assembly jobs to the U.S. while the manufacturing, technology, and R&D stay in China. Today and for the foreseeable future, no American company makes transit rail cars, but the evidence is compelling that the Chinese government has now directed state-owned entities to target the U.S. freight rail manufacturing sector as well. Our freight railcar industry is now in China's sights.

As our nation's freight railcar manufacturers continue to incorporate innovative new technologies to enhance the safety and productivity of our rail system, the growing presence of China's CRRC is all the more concerning. From rural communities to major cities to seaports and government installations,

freight rail not only serves as the primary mode of transport for an array of key products and commodities, but also for sensitive U.S. military equipment, hazardous nuclear waste, and toxic chemicals. We must take urgent measures to ensure freight rail remains secure and American-run. We must retain the know-how and technology to improve our rail system in the future, and safeguard against disruption of this strategically vital sector of our economy and pillar of our national security.

# Endnotes


1 Oxford Economics, "Will We Derail U.S. Freight Rolling Stock Production," May 2017. https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production
2 Federal Railroad Administration, "National Rail Plan Progress Report", September 2010. Cited in https://www.fra.dot.gov/page/P0362
3 Towson University, Regional Economic Studies Institute, June 2016 (quoted in AAR President Ed Hamberger's April 11, 2018 Statement to the House Appropriations Committee THUD Subcommittee hearing on Rail Safety, and Infrastructure).
4 Federal Register, "Indexing the Annual Operating Revenues of Railroads," Cited in https://www.fra.dot.gov/page/P0362
5 Federal Railroad Administration, 'Freight Rail Background," March 2012. Cited in https://www.fra.dot.gov/page/P0362
6 Department of Homeland Security, "Transportation Systems Sector." https://www.dhs.gov/transportation-systems-sector
7 Oxford Economics, "Will We Derail U.S. Freight Rolling Stock Production," May 2017. https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production
8 Towson University, Regional Economic Studies Institute, June 2016 (quoted in AAR President Ed Hamberger's April 11, 2018 Statement to the House Appropriations Committee THUD Subcommittee hearing on Rail Safety, and Infrastructure).
9 Federal Railroad Administration, "National Rail Plan Progress Report," September 2010. Cited in https://www.fra.dot.gov/page/P0362
10 Federal Railroad Administration, "Freight Rail Overview," https://www.fra.dot.gov/page/P0362
11 Louisiana Department of Transportation & Development, "A Comparative Analysis of Intermodal Ship-to-Rail Connections at Louisiana Deep Water Ports," August 2007. http://wwwsp.dotd.la.gov/Inside_LaDOTD/Divisions/Multimodal/Marine_Rail/Misc%20Documents/A%20Comparative%20Analysis%20of%20Intermodal%20Ship%20to%20Rail%20Connections%20at%20Louisiana%20Deep%20Water%20Ports.pdf
12 As Prepared Remarks of Ronald L. Batory Swearing-In Ceremony as the 14th Administrator of the
Federal Railroad Administration, U.S. Department of Transportation Headquarters, Washington, DC, February 28, 2018. https://www.fra.dot.gov/Elib/Document/17848
13 The Made in China 2025 plan identifies ten priority sectors: next-generation information technology; high-end numerical control machinery and robotics; aerospace and aviation equipment; maritime engineering equipment and high-tech maritime vessel manufacturing; advanced rail equipment; energy-saving and new energy vehicles; electrical equipment; new materials; biomedicine; and agricultural machinery.
14 White House Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," June 2018. https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf
15 CRRC 2016 Annual Report, April 2017. http://www.hkexnews.hk/listedco/listconews/SEHK/2017/0427/LTN201704272466.pdf
16 "CRRC Corporation Limited Articles of Association," CRRC Corporation Limited, at 70. http://www.crrcgc.cc/Portals/73/Uploads/Files/2018/6-4/636637164457871915.pdf
17 "America's most expensive weapons system, the F-35, is a key symbol of Trump's trade gripe with China," CNBC, March 22, 2018 https://www.cnbc.com/2018/03/22/americas-most-expensive-weapons-system-the-f-35-is-a-key-symbol-of-trumps-trade-gripe-with-china.html
18 "Chinese Nationals Stole Marine Technology to Benefit Chinese Regime, According to US Justice Department," Epoch Times, April 30, 2018. https://www.theepochtimes.com/chinese-nationals-stole-marine-technology-to-benefit-chinese-regime-according-to-u-s-justice-department_2509135.html
19 "United States Imposes Sanctions Against Chinese Firm," Nuclear Threat Initiative, September 22, 2004. https://www.nti.org/gsn/article/united-states-imposes-sanctions-against-chinese-firm/
20 "CRRC 2016 Annual Report," CRRC Corporation Limited, April 28, 2017 http://www.crrcgc.cc/Portals/73/Uploads/Files/2017/4-28/636289739063167304.pdf
21 Focusing initially with transit freight contracts allowed CRRC the opportunity to work with local governments and small businesses, leveraging CRRC's economies of scale at a much lower level than were CRRC to initially tackle the larger-scale, higher visibility, more stringent review process associated with freight rail contracts.
22 "China-based T supplier keeps rolling," CommonWealth, March 24, 2017. https://commonwealthmagazine.org/politics/china-based-t-supplier-keeps-rolling/
23 Oxford Economics, "Will We Derail U.S. Freight Rolling Stock Production," May 2017. https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production
24 William Vantuono, "New tank car builder coming on line," Railway Age, February 13, 2014. https://www.railwayage.com/financeleasing/new-tank-car-builder-coming-on-line/
25 "CRRC to build North American wagon plant in Canada," Railway Gazette, May 5, 2017. http://www.railwaygazette.com/news/news/n-america/single-view/view/crrc-to-build-north-american-wagon-plant-in-canada.html
26 Letter from Rail Security Alliance to U.S. Trade Representative, December 14, 2017.
27 @CRRC_global, "Following CRRC's entry to Jamaica, our products are now offered to 104 countries and regions. So far, 83% of all rail products in the world are operated by #CRRC or are CRRC ones. How long will it take for us conquering the remaining 17%?" Twitter, January 11, 2018. https://twitter.com/CRRC_global/status/951476296860819456
28 Yosi Melman, "Cause for Concern? Chinese Investment and Israel's National Security," The Jerusalem Post, April 7, 2018. https://www.jpost.com/Jerusalem-Report/Chinese-TAKEAWAY-546692
29 Hermine Donceel and Eric Maurice, "EU Parliament approves new anti-dumping methodology," EU Observer, November 15, 2017. https://euobserver.com/economic/139866
30 David Morris, "Railroad Association Denies Smart Train Cyber Vulnerabilities," Fortune, January 22, 2016. http://fortune.com/2016/01/22/railroad-association-denies-smart-train-cyber-vulnerabilities/
31 Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," The New York Times, July 8, 2018. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html
32 Sophie Curtis, "Spy agencies 'ban Lenovo from secret networks," The Telegraph, July 29, 2013. https://www.telegraph.co.uk/technology/news/10208578/Spy-agencies-ban-Lenovo-from-secret-networks.html
33 Alwyn Scott, "China drone maker steps up security after U.S. Army ban," Reuters, August 14, 2017. https://www.reuters.com/article/us-usa-drones-dji/china-drone-maker-steps-up-security-after-u-s-army-ban-idUSKCN1AU294
34 Max Greenwood, "US Army base removes Chinese-made surveillance cameras," The Hill, January 12, 2018. http://thehill.com/policy/defense/368710-us-army-base-removes-chinese-made-surveillance-cameras
35 Hamza Shaban, "Pentagon tells U.S. military bases to stop selling ZTE, Huawei phones," The Washington Post, May 2, 2018. https://www.washingtonpost.com/news/the-switch/wp/2018/05/02/pentagon-tells-u-s-military-bases-to-stop-selling-zte-huawei-phones/?utm_term=.bf1e99041b11
36 Keith Stouffer et al. "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-2, Revision 2, May 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
37 "The state of cybersecurity in the rail industry," Rockwell Collins, August 2017. https://www.rockwellcollins.com/-/media/Files/rc2016/marketing/C/Cybersecurity-solutions/The-state-of-cybersecurity-in-the-rail-industry-white-paper.pdf?lastupdate=20171215210046

38 J. William Middendorf II and Dan Negrea, "China takes a wrong turn," The Washington Times, March 11, 2018. https://www.washingtontimes.com/news/2018/mar/11/china-takes-a-wrong-turn/
39 Testimony of Michael T. Haley, "Update on Federal Rail and Public Transportation Security Efforts," Hearing before the Subcommittee on Transportation Security and Infrastructure Protection, of the Committee on Homeland Security, U.S. House of Representatives, February 6, 2007.
40 "Transportation Sector-Specific Plan: Freight Modal Annex," U.S. Department of Homeland Security, 2007, Pg. 2. https://www.hsdl.org/?view&did=474331
41 "Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience," The White House, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
42 Government Accountability Office, "Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored," Report No. 09-243, April, 2009, Pg. 7. https://www.gao.gov/products/GAO-09-243
43 Id at 7.
44 Testimony of Michael T. Haley, "Update on Federal Rail and Public Transportation Security Efforts," Hearing before the Subcommittee on Transportation Security and Infrastructure Protection, of the Committee on Homeland Security, U.S. House of Representatives, February 6, 2007.
45 "Strategic Rail Corridor Network (STRACNET)," Global Security, 2012. https://www.globalsecurity.org/military/facility/stracnet.htm
46 Id.
47 "About SDDC," U.S. Army Military Surface Deployment and Distribution Command, 2016. https://web.archive.org/web/20110818114337/http://www.sddc.army.mil/What/default.aspx
48 James Jackson, "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service, July 3, 2018. https://fas.org/sgp/crs/natsec/RL33388.pdf
49 Executive Order No. 13788, "Buy American and Hire American," April 18, 2017. https://www.whitehouse.gov/presidential-actions/presidential-executive-order-buy-american-hire-american/