**Prepared Statement of**
**Brigadier General John Adams, U.S. Army (Retired)**
**President, Guardian Six LLC**

**House Committee on Transportation and Infrastructure**

**"The Impacts of State-Owned Enterprises on Public Transit and Freight Rail Sectors"**

**May 16, 2019**

***Introduction***

Chairman DeFazio, Ranking Member Graves, and members of the Committee, I want to thank you for inviting me to testify at this critically important hearing on securing our freight and transit rail sectors against Chinese state-owned enterprises (SOE). My name is John Adams and I am a 30-year veteran of the US Army and President of Guardian Six LLC, (Guardian). Guardian Six is a defense and national security consulting firm, which specializes in understanding, assessing, and mitigating against national security threats to our Nation's defense industrial base. Guardian Six is also a national security advisor to the Rail Security Alliance (RSA) which is a coalition of North American freight railcar manufacturers, suppliers, steel interest and unions committed to ensuring the economic and national security of our freight and transit rail systems. Notably, on October 22, 2018, Guardian Six published a report titled "National Security Vulnerabilities of the U.S. Freight Rail Infrastructure and Manufacturing Sector – Threats and Mitigation," which systematically examines, among other things, the threats posed by SOEs in this industry.

Our country depends upon the freight rail system to provide safe, reliable, and effective transportation for our defense and homeland security infrastructure. I know first-hand that our national survival depends upon these vital rail links as the primary transportation for U.S. military equipment, infrastructure logistics, hazardous waste, toxic substances, and the range of products and commodities that support our entire economy. U.S. freight rail is a strategic asset, the health and integrity upon which our armed forces depend to maintain readiness and preserve our defense capacity. Our freight rail system connects ports to rural and urban inland hubs, military bases to each other, and to key logistics nodes throughout our Nation. It also links the U.S. by land to key allies and trading partners Canada and Mexico and enables transportation between coastal and inland military and homeland infrastructure nodes. On the passenger side,

millions of Americans rely on transit rail systems every day. The U.S. rail system is also highly sophisticated, relying on a constantly expanding network of technology and digitization that dramatically increases its risk to cyber-attack and hacking.

Today, I would like to draw the Committee's attention to China's strategic targeting of the U.S. rail manufacturing sector, with aggressive, strategic and anti-competitive actions. China is making substantial economic inroads into our rail system's supporting supply chains, as well as rolling stock asset ownership and management. Beijing's 2015 "Made in China 2025" plan leverages state resources and industrial policy, specifically aiming for a comparative advantage in the global advanced rail sector among nine other sectors. China's strategy to capture the U.S. rail system's supply chain threatens the system's cyber-security, reliability, and safety. Any Chinese dominance of the U.S. rail system would turn the system from a bedrock strategic asset into a potentially crippling vulnerability.

***China's State-Owned Enterprises Target U.S. Rail Manufacturing***

The United States has seen a growth in Chinese foreign direct investment over the last few decades, exceeding $140 billion in 2018.[1] Much of this investment is targeted in several sectors including energy, telecommunications, and transportation – industries that make up key pillars of our country's critical infrastructure. In the rail transportation sector, this investment has been spearheaded by a Chinese SOE called the China Railway Rolling Stock Corporation (CRRC). Specifically, CRRC is a massive conglomerate that is wholly owned by the Chinese government, with deep ties to the Communist Party of China. Not only does CRRC possess 90 percent of China's domestic market to produce rail locomotives, bullet trains, passenger trains and metro vehicles, but it has dramatically and strategically increased its investment and footprint in the United States. This fact raises serious questions and concerns about the current and future safety and security of our Nation's railroads.

[1] Rhodium Group, *China Investment Monitor: Capturing Chinese Foreign Investment Data in Real Time*. https://rhg.com/impact/china-investment-monitor/

The "Made in China 2025" initiative, a key component of China's 13th Five-Year plan,[2] identifies the rail manufacturing sector as a top target for Chinese expansion. This initiative has systematically and deliberately driven strategic investment and financing activities of the SOE CRRC in third-country markets and the United States.[3] In 2015, CRRC reported revenues of more than $37 billion[4] — significantly outpacing the entire U.S. railcar market, which had $22 billion of output during the same year.[5] According to Chinese state media, CRRC plans to increase overseas sales to $15 billion by next year alone. This represents about double the level of export orders from just four years ago[6] and according to CRRC's own presentation materials the U.S. market remains a prime target to, as they put it, "conquer."[7]

CRRC's bylaws direct that the company seek guidance from the Communist Party of China on significant matters affecting the company's operations.[8] Three of CRRC's current board members previously held high-level positions at several state-owned defense companies including, 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.

---

[2] U.S.-China Economic and Security Review Commission, *2016 Report to Congress*, November 2016, at 100.
[3] Langi Chiang, *China's largest train maker CRRC Corp announces 12.2 billion yuan in contracts*, South China Morning Report, July 23, 2015. https://www.scmp.com/business/companies/article/1842983/chinas-largest-train-maker-crrc-corp-announces-122-billion-yuan
[4] CRRC Corporation, 2015 CRRC Annual Report, https://www.crrcgc.cc/Portals/73/Uploads/Files/2016/8-23/636075436968234671.pdf
[5] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?* May 2017, at 24.
[6] Brenda Goh, *China Trainmaker CRRC to build more plants abroad in expansion plan: China Daily*, REUTERS, Dec. 5, 2016, http://www.reuters.com/article/us-crrc-expansion-idUSKBN13U0EJ
[7] @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. [Tweet deleted]
[8] "CRRC Corporation Limited Articles of Association," CRRC Corporation Limited, at 70. http://www.crrcgc.cc/Portals/73/Uploads/Files/2018/6-4/636637164457871915.pdf

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 link between CRRC board members and these compromising activities. Coupled with these facts, 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.[9] 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 company.[10] NORINCO has also been sanctioned by the U.S. State Department on six occasions for contributing to Iranian Weapons of Mass Destruction (WMD) development.[11] 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.

Using state-backed financing, subsidies, and an array of other government resources, CRRC has strategically targeted and sought to capture the U.S. railcar manufacturing sector. In just the last five years the United States has witnessed CRRC establish rail assembly operations for transit railcars in two states, along with additional research and bidding operations in several others. By beginning with a business strategy to take market share in the U.S. transit rail manufacturing sector and deploying near-limitless financing from its home government to help ensure the well below-market bids for new U.S. metropolitan transit projects, CRRC has quickly established itself as a formidable force and major competitor in the U.S. transit rail system..

Thus far China has secured four U.S. metropolitan transit contracts, totaling $2.6 billion, largely by utilizing anticompetitive under-bidding practices. In each case, CRRC leveraged massive subsidies and other resources from the Chinese government to dramatically underbid its competitors, and in one case going as much as fifty percent below the bid submitted by another

[9] "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

[10] "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

[11] "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/

competitor. The trains purchased by those U.S. metropolitan transit agencies will contain Wi-Fi systems, automatic train control, automatic passenger counters, surveillance cameras, and the Internet of Things (IoT) technology that will be thoroughly integrated into the information and communications technology infrastructure of transit authorities, all designed and built by the Government of China.

The fact that the advanced technologies in these trains is sole-sourced from a Chinese state-owned enterprise is alarming and the risk is very high that Chinese-built-in surveillance cameras could track the movements and routines of passengers, searching for high-value targets that intelligence officials can then identify to vacuum data from using the train's built-in Wi-Fi systems. Some argue that these risks are low and manageable; however, I beg to differ. Already, China is openly developing a system of "algorithmic surveillance" that leverages advances in artificial intelligence and facial recognition technology to enable the Chinese Communist Party to monitor the movements and patterns of its own citizens, purportedly as a means of combatting crime. China boasts about how it has utilized the latest advances in Artificial Intelligence (AI) and facial recognition technology to identify and track its 1.4 billion citizens,[12] creating a very real prospect that they have the current capacity and interest in doing the same here, in the United States.

Several recent cases involving CRRC bids for new transit rail projects serve as compelling examples of the strategy being employed by China to capture our rail systems. For example:

- CRRC bid $567 million to win a contract with the Massachusetts Bay Transit Authority (MBTA) in Boston in 2014, coming as much as 50 percent below other bidders.[13]
- CRRC won a 2016 contract to provide transit rail for the Chicago Transit Authority (CTA), bidding $226 million less than the next-highest bidder.[14]

[12] Surveillance Cameras Made by China Are Hanging All Over the U.S., The Wall Street Journal, November 12, 2017. https://www.wsj.com/articles/surveillance-cameras-made-by-china-are-hanging-all-over-the-u-s-1510513949
[13] Bonnie Cao, *After Winning MBTA Contract, China Trainmaker CRRC Plans American Expansion*, Boston Globe, Sept. 11, 2015. https://www.bostonglobe.com/business/2015/09/11/after-winning-mbta-contract-china-trainmaker-crrc-plans-american-expansion/jnS1kU7uHWFGR9gjWmDEjM/story.html
[14] Corilyn Shropshire, *First Step to New CTA Rail Cars: Build the Factory in Chicago*, Chicago Tribune, Mar. 16, 2017. http://www.chicagotribune.com/business/ct-cta-new-railcar-plant-0316-biz-20170315-story.html

- CRRC bid $137.5 million in 2017 for a contract with Southeastern Pennsylvania Transportation Authority (SEPTA) in Philadelphia, underbidding the next-lowest bidder—which had a robust local manufacturing presence—by $34 million.[15]
- CRRC finalized a contract with the Los Angeles County Metropolitan Transportation Authority in 2017 for its transit rail system worth up to $647 million.[16] Again, China did this by leveraging below-market financing, which in turn undercut other bidders.

Emboldened with these contract victories, CRRC continues to target other U.S. cities, including our nation's capital. In September, the Washington Metropolitan Transit Authority (WMATA), which is the second largest mass transit system in the country, issued a Request for Proposals (RFP) for the new 8000-series metro car. This RFP includes video surveillance, monitoring and diagnostics, data interface with WMATA, and automatic train control systems that are susceptible to cyber-attacks. In response to concerns expressed by a number of lawmakers, including the Vice Chairman of the Senate Intelligence Committee, WMATA re-issued its RFP to include additional cybersecurity protections.[17]

Most concerning is that whomever is selected to supply railcars for WMATA will become a partner in the day-to-day operations of a Metro system whose stops include the Pentagon and the Capitol, as well as unfettered access to our Nation's tunnels and underground infrastructure. We couple this reality with two additional critical facts. First, a classified report written by WMATA's Inspector General recently concluded that there were significant shortcomings in WMATA's enterprise-level cybersecurity posture.[18] Second, the New York Times recently noted that "businesses and government agencies in the United States have been targeted in aggressive attacks by…Chinese hackers…"[19] So, in light of China's pervasive history of cyber

[15] Jason Laughlin, *Mass.-Based Company with Chinese Backing Beats Local Group for SEPTA Car Contract*, The Philadelphia Inquirer, Mar. 21, 2017. http://www.philly.com/philly/business/transportation/Mass-based-company-with-Chinese-backing-beats-out-local-group-for-SEPTA-car-contract.html
[16] Keith Barrow, *Los Angeles Orders CRRC Metro Cars*, International Railway Journal, Mar. 24, 2017. http://www.railjournal.com/index.php/north-america/los-angeles-orders-crrc-metro-cars.html
[17] Sean Lyngaas, D.C. Metro system beefs up supply-chain cybersecurity provisions for new railcars, Cyberscoop, February 6, 2019. https://www.cyberscoop.com/metro-dc-subway-cyberscecurity-rfp/
[18] Ryan Johnston, D.C. Metro needs to improve its cybersecurity, audit finds, Statescoop, July 9, 2018. https://statescoop.com/wmata-incident-response-audit-calls-for-improved-cybersecurity-plan/
[19] Nicole Perlroth, Chinese and Iranian Hackers Renew Their Attacks on U.S. Companies, New York Times, February 18, 2019. https://www.nytimes.com/2019/02/18/technology/hackers-chinese-iran-usa.html

espionage and hacking, we cannot trust a Chinese SOE to build, own, or operate U.S. critical infrastructure.

As troubling as these developments in our transit rail sector are, they are even more alarming because they provide CRRC the opportunity to pivot into freight rail assembly, a subsector of rail not protected by the same Buy America requirements as transit rail, and one that represents a dangerous vulnerability if overtaken by the Government of China. 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. With 140,000 miles of rail lines across the United States, the North American freight rail system transports five million tons of goods and materials each day. By providing a means for safe, reliable and effective transportation, freight rail keeps our nation's economy thriving while helping to ensure the security of our homeland. Penetrating our freight rail market will allow China to 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 its own employment base.

CRRC is making steady and deliberate headway into the freight rail sector with the launch of Vertex Rail Corporation and American Railcar Services. Vertex Rail Corporation is now a defunct freight rail assembly facility that was based in Wilmington, North Carolina. On the other hand, American Railcar Services is a separate assembly facility headquartered in Miami, Florida, that maintains assembly operations in Moncton, New Brunswick.

Concerns about CRRC's transition into freight rail manufacturing are best illustrated by the recent experiences of third-country markets like Australia, whose freight rail manufacturing sector CRRC entered in 2008. In less than ten years, CRRC effectively decimated the sector, forcing the four domestic suppliers out of business and out of the rail market which left only CRRC standing. Today, almost no meaningful Australian passenger or freight rolling stock manufacturing exists – CRRC's Australia footprint is almost exclusively that of an assembler of Chinese-made parts and a financier of purchases from CRRC. That cannot happen here.

***National Security Implications***

As stated earlier in my testimony, the threat of Chinese dominance of our freight and transit rail sectors is more than just a market concern. The Department of Defense (DoD) has a longstanding reliance on freight rail in the United States. Unlike the U.S. maritime shipping industry, whose security is protected by the Jones Act, a measure that requires vessels transporting goods between U.S. ports to be U.S.-built and majority U.S.-owned, freight rail in America has been left comparatively unprotected. Yet, the Department of Homeland Security (DHS) deems the U.S. rail sector as part of the nation's critical infrastructure,[20] noting that 140,000 rail miles enable U.S. freight rail to run through every major American city and every military base in the nation. 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.[21] The DOD's Military Traffic Management Command (MTMC) has designated nearly 40,000 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. 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.

Freight rail is also core to 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), a component of TRANSCOM, operates 10,000 containers and some 1,350 rail cars to deliver equipment and supplies for deployed members of the Army, Navy, Air Force, Marines, and Coast Guard. SDCC also leverages commercial freight rail to provide important components of DoD's surface

[20] Presidential Policy Directive 21 (PPD-21) identifies 16 critical infrastructure sectors, including "Transportation Systems." The Department of Homeland Security defines "Freight Rail" as one of the seven key subsectors. *See generally*, PPD-21, *Critical Infrastructure Security and Resilience*, Feb. 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil and *Transportation Systems Sector*, Dep't of Homeland Sec., Mar. 25, 2013, http://www.dhs.gov/transportation-systems-sector

[21] "Strategic Rail Corridor Network (STRACNET)," Global Security, 2012. https://www.globalsecurity.org/military/facility/stracnet.htm

transportation requirements.[22] SDCC uses a fleet of 1,850 specially designed heavy-duty flatcars managed by a company owned by the major freight railroads.

The specter of Chinese dominance over our freight rail system presents a myriad of national security concerns. The 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 transports most of our t nuclear waste and hazardous material. 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 that disturbance is undetected, a release of toxic chemicals could have catastrophic consequences and cost American lives. Moreover, Chinese intelligence about U.S. rail freight logistical movements could provide China with a destabilizing economic competitive edge. Last and certainly not least, Chinese access to U.S. freight rail would also mean that the risk of malicious intrusions into our rail infrastructure, including those carried out by terrorists, would become more difficult for U.S. operators to detect or counter.

Predatory Chinese efforts to penetrate our freight rail market also 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.

[22] "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

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.[23]

As noted in my 2018 report on the vulnerabilities of freight rail,[24] our rail system's rapidly expanding IoT capabilities present an array of national security challenges that include:

- **Digitized railroad network/IoT:** Integrated teams of data scientists, software developers, and engineers develop and apply technology across every aspect of the nationwide freight rail network, effectively increasing the vulnerability of industrial control systems, train operations, and perhaps even the industry's metadata warehousing centers to cyber threats.
- **Rail Signaling:** Congress has mandated the installation of positive train control (PTC) systems on much of the nation's rail systems as a means of preventing specific accidents. A malicious cyber breach of PTC or underlying existing rail signaling systems could wreak havoc and cause accidents or derailments on the highly interdependent freight railway network.
- **Locomotives:** Rail locomotives rely upon hundreds of sensors to monitor asset health and performance of train systems.
- **Onboard Freight Car Location & Asset Health Monitoring:** Thousands of freight cars are equipped with telematics or remote monitoring equipment, many of which are carrying hazardous materials like chlorine, anhydrous ammonia, ethylene oxide, and flammable liquids. This tracking technology includes a wireless communication management unit to track precise near-real time location via GPS, direction of travel, speed, and dwell time within the Transportation Security Administration (TSA)'s 45 designated high-threat urban areas (HTUAs).[25]

---

[23] 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

[24] *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.

[25] 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.

- **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 that tracks GPS location and can allow a locomotive engineer to initiate an emergency brake application, a critical safety feature for trains that can stretch upwards of 10,000 feet long.

The presence of these evolving technologies underscores the clear danger of a foreign country, and particularly the Government of China and its SOEs, having unfettered control of freight manufacturing in the U.S. market. Already, there are reports of Chinese manufacturers investigating the production of their own "telematics" technology to allow the monitoring and control of their rail cars.[26]

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, it is equally important that policymakers enact legislation directed to stop immediately the scope and impact of China's ongoing incursion into an increasingly digitized rail network.

***Mitigation***

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.

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

[26] *China plans 'smart trains' to take on global rail companies*, CHINA DAILY, March 10, 2016, page 1 http://english.chinamil.com.cn/news-channels/2016-03/10/content_6952271_2.htm

measures have included a reported U.S. government ban on the purchase of Chinese drones[27] and the removal of Chinese-made security cameras from U.S. military bases.[28] In April 2018, DoD reportedly also banned Huawei and ZTE cell phones from sale in U.S. military exchanges world-wide.[29] We have yet to do the same to protect Chinese incursions into the U.S. freight rail manufacturing base.

While there is no single solution that will mitigate the concerns and risks described in my testimony today, I suggest that we must modernize our national policies to reflect these security risks. It is difficult to overstate the potential impact on our national security and our economic future if we do not take a comprehensive and long-range approach to CRRC specifically, and SOEs generally.

Considering these security risks, both chambers of Congress last year attempted to pass a ban on federal funding going to CRRC through the appropriations process. This year 30 Senators have so far signed onto legislation that would place a permanent ban on Federal funding going to CRRC and the House just recently introduced a bill as well. I would urge members of this Committee to join their colleagues in co-sponsoring the Transit Infrastructure Vehicle Security Act. Congress also passed legislation last year that would mandate DHS, in coordination with the Committee on Foreign Investment in the United States and the Department of Transportation, to produce a report on the national security threats of Chinese SOE investment in our rolling stock manufacturing sector.[30]

It is now time for our Nation's leaders to put an end to CRRC's infiltration of the U.S. rail manufacturing industry by developing comprehensive restrictions to ensure the integrity of our

[27] 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
[28] 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
[29] 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
[30] See. H.R.5515 - John S. McCain National Defense Authorization Act for Fiscal Year 2019, Sec. 1719(c)

Nation's transportation systems. In that vein, I recommend that Congress and the Administration giver serious and immediate consideration to:

- Developing comprehensive restrictions and additional reviews on investments from SOEs in critical infrastructure integral to our national defense.
- Ensuring 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-owned entities.
- Strengthening 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.

***Conclusion***

We need urgent action to safeguard our U.S. rail system's health and integrity. Chinese control of our rail system's supply chains, much less control of the system through cyber-intrusion or outright firm ownership, threatens this vital national security asset. The strategic targeting of our Nation's infrastructure by the Government of China and its state-owned enterprises poses a fundamental threat to the fabric of our critical infrastructure and is a pressure point for malicious cyber actors to threaten not only the economic and national security of the United States, but to our standing as a global power.

We greatly appreciate the Committee's interest in addressing these critical issues. We must take action to safeguard our U.S. rail system's health and integrity before we lose it. We owe it to the American people to ensure that the American freight rail sector continues to be a vibrant and secure element of our Nation's infrastructure, keeping us safe and carrying our economy into the future.

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