Prepared Statement of
Erik R. Olson
Vice President
Rail Security Alliance

House Committee on Homeland Security

Subcommittee on Transportation and Maritime Security
Subcommittee on Cybersecurity, Infrastructure Protection and Innovation

"Securing U.S. Surface Transportation from Cyber Attacks"

February 26, 2019

Introduction

Chairman Correa, Chairman Richmond, Ranking Member Lesko, Ranking Member Katko, and members of the Subcommittees, my name is Erik Olson and I am the Vice President of the Rail Security Alliance. The Rail Security Alliance is a coalition of North American freight railcar manufacturers, suppliers, unions, and steel interests committed to ensuring the economic and national security of our passenger and freight rail systems. On behalf of our coalition, thank you for the opportunity to testify on the critical topic of securing our surface transportation systems against cyber and privacy threats.

Rail in the United States is an integral component of our critical infrastructure and our way of life. With nearly 140,000 miles of railroad covering the United States, freight rail regularly transports key commodities, sensitive U.S. military equipment, hazardous waste, potentially toxic and hazardous chemicals, and flammable liquids across the country every day. On the passenger side, millions of Americans rely on commuter 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 want to draw the Committee's attention to a particular threat arising from foreign investment in this industry that jeopardizes the future of America's passenger and freight rail systems. China is strategically targeting the U.S. rail manufacturing sector, with aggressive, strategic and anticompetitive actions. Thus far they have secured four U.S. metropolitan transit contracts, largely by utilizing anticompetitive under-bidding practices. With China's government picking up U.S. transit rail manufacturing contracts, the Chinese are now using their rail manufacturing capabilities to assail the U.S. freight manufacturing sector in a move that is reminiscent of what has already occurred in third country markets such as Australia. This activity is a pattern for China's state-owned rail sector and raises grave national security concerns. Without action, America's industrial, military, and other government interests could be forced to

rely significantly or wholly on rail cars made by the Chinese Government, thus creating massive cyber vulnerabilities that threaten our military and industrial security.

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

The "Made in China 2025" initiative, a key component of China's 13th Five-Year plan,[1] 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 state-owned China Railway Rolling Stock Corporation (CRRC) in third-country markets and the United States. CRRC is wholly owned by the Government of China and it has 90 percent of China's domestic market for production of rail locomotives, bullet trains, passenger trains and metro vehicles.[2] In 2015, CRRC reported revenues of more than $37 billion[3] — significantly outpacing the entire U.S. railcar market, which had $22 billion of output during the same year.[4] 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[5] and according to CRRC's own presentation materials the U.S. market remains a prime target to, as they put it, "conquer."[6]

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 5 years the United States has witnessed CRRC establish rail assembly operations for transit railcars in three 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 lower the well below-market bids for new U.S. metropolitan transit projects, CRRC has quickly established itself as a formidable force in U.S. transit rail competition.

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:

---

[1] U.S.-China Economic and Security Review Commission, *2016 Report to Congress*, November 2016, at 100.
[2] 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
[3] CRRC Corporation, 2015 CRRC Annual Report, https://www.crrcgc.cc/Portals/73/Uploads/Files/2016/8-23/636075436968234671.pdf
[4] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?*, May 2017, at 24.
[5] 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.
[6] @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

- CRRC bid $567 million to win a contract with the Massachusetts Bay Transit Authority (MBTA) in Boston in 2014, coming in roughly50 percent below other bidders.[7]
- In 2016, CRRC won a contract to provide transit rail for the Chicago Transit Authority (CTA), bidding $226 million less than the next-highest bidder.[8]
- In early 2017, CRRC bid $137.5 million 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.[9]
- In March 2017, CRRC finalized a contract with the Los Angeles County Metropolitan Transportation Authority for its transit rail system worth up to $647 million.[10] Again, China did this by leveraging below-market financing, which in turn undercut other bidders.

Emboldened with these contract wins, 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.[11]

But the Rail Security Alliance's concerns do not end there. 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.[12] Second, just last week the New York Times

---

[7] 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

[8] 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

[9] 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

[10] 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

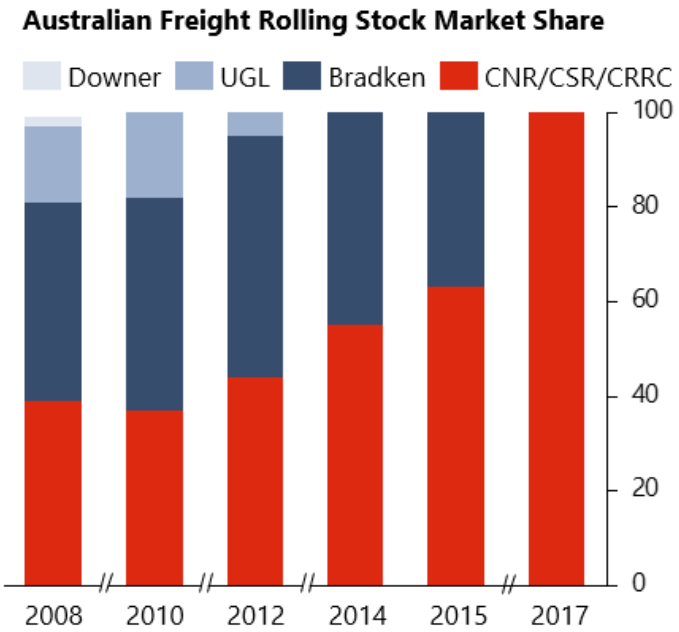
[11] Sean Lyngaas, D.C. Metro system beefs up supply-chain cybersecurity provisions for new railcars, Cyberscoop, February 6, 2019. https://www.cyberscoop.com/metro-dc-subway-cyberscecurity-rfp/

[12] 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/

noted that "businesses and government agencies in the United States have been targeted in aggressive attacks by…Chinese hackers… ."[13] So, in light of China's pervasive history of cyber espionage and hacking, it is the position of the Rail Security Alliance that we cannot trust a Chinese state-owned enterprise to build, own, or operate in U.S. critical infrastructure.

These developments 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 troubling vulnerability if overtaken by the Government of China. Even so, CRRC is making steady and deliberate headway into this 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, FL 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 10 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. We cannot let that happen here.



Source: Oxford Economics; RSA internal data

Implications for National Security

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,[14] noting that 140,000 rail miles enable U.S. freight rail to run through

[13] 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

[14] 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-

every major American city and every military base in the nation. The Department of Defense (DoD), which itself maintains a fleet of more than 1,300 rail cars, has also designated nearly 40,000 miles of freight rail as part of the Strategic Rail Corridor Network (STRACNET), a comprehensive rail network that connects military bases and maritime ports across the country.[15] We have had extensive discussions with representatives from the Department of Defense, and based on those discussions I am confident that the Secretary of Defense would express his concerns on this matter as well.

Because freight rail transports not only military freight and industrial products, but also nuclear material and hazardous chemicals that can be safely and effectively transported only by rail, there is a serious risk that the technologies in these systems could be compromised by a malicious actor. As noted by Brig. Gen. John Adams (USA, Ret.) in a 2018 report on the vulnerabilities of freight rail[16], our rail system's rapidly expanding Internet of Things (IoT) capabilities presents an array of national security challenges that include:

- **A digitized railroad network/the Internet of Things:** 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

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.

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

[16] 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

within the Transportation Security Administration (TSA)'s 45 designated high-threat urban areas (HTUAs).[17]

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 (See Attachment A).

The presence of these evolving technologies underscores the clear danger of a foreign country, and particularly the Government of China and its state-owned enterprises, having undue 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.[18] On the transit side, China is already boasting about how it has utilized the latest advances in AI and facial recognition technology to identify and track its 1.4 billion citizens,[19] creating a very real prospect that they could do the same here in the United States.

Conclusion

As China's CRRC becomes more dominant as a U.S. rail manufacturer, there are urgent and compelling questions we must answer regarding whether a growing presence of, and reliance upon freight or passenger cars from a major state-owned Chinese rail enterprise is likely to compromise the security and safety of industrial, military, and civilian transportation systems in the United States. For that reason, we are grateful that Congress passed legislation last year that would mandate the Department of Homeland Security, in coordination with the Committee on Foreign Investment in the United States and the Department of Transportation, produce a report on the national security threats of Chinese SOE investment in our rolling stock manufacturing sector,[20] and we strongly urge the Committee to work with DHS as that report is completed.

We greatly appreciate the Committee's interest in addressing these critical issues. 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.

Thank you again for the opportunity to testify. I look forward to answering any questions you may have.

---

[17] 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.

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

[19] 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

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