

THREATS POSED BY STATE-OWNED AND  
STATE-SUPPORTED ENTERPRISES TO PUBLIC  
TRANSPORTATION

---

HEARING  
BEFORE THE  
COMMITTEE ON  
BANKING, HOUSING, AND URBAN AFFAIRS  
UNITED STATES SENATE  
ONE HUNDRED SIXTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING THE THREATS POSED BY STATE-OWNED AND STATE-  
SUPPORTED ENTERPRISES TO PUBLIC TRANSPORTATION

---

MARCH 5, 2020

---

Printed for the use of the Committee on Banking, Housing, and Urban Affairs



Available at: <https://www.govinfo.gov/>

---

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama	SHERROD BROWN, Ohio
PATRICK J. TOOMEY, Pennsylvania	JACK REED, Rhode Island
TIM SCOTT, South Carolina	ROBERT MENENDEZ, New Jersey
BEN SASSE, Nebraska	JON TESTER, Montana
TOM COTTON, Arkansas	MARK R. WARNER, Virginia
MIKE ROUNDS, South Dakota	ELIZABETH WARREN, Massachusetts
DAVID PERDUE, Georgia	BRIAN SCHATZ, Hawaii
THOM TILLIS, North Carolina	CHRIS VAN HOLLEN, Maryland
JOHN KENNEDY, Louisiana	CATHERINE CORTEZ MASTO, Nevada
MARTHA MCSALLY, Arizona	DOUG JONES, Alabama
JERRY MORAN, Kansas	TINA SMITH, Minnesota
KEVIN CRAMER, North Dakota	KYRSTEN SINEMA, Arizona

GREGG RICHARD, *Staff Director*

LAURA SWANSON, *Democratic Staff Director*

JEN DECI, *Professional Staff Member*

HOMER CARLISLE, *Democratic Professional Staff Member*

CAMERON RICKER, *Chief Clerk*

SHELVIN SIMMONS, *IT Director*

CHARLES J. MOFFAT, *Hearing Clerk*

JIM CROWELL, *Editor*

# C O N T E N T S

THURSDAY, MARCH 5, 2020

	Page
Opening statement of Chairman Crapo .....	1
Prepared statement .....	29
Opening statements, comments, or prepared statements of:	
Senator Brown .....	2
Prepared statement .....	29

## WITNESSES

Senator Tammy Baldwin of Wisconsin .....	5
Prepared statement .....	31
Senator John Cornyn of Texas .....	11
Prepared statement .....	32
E. Michael O'Malley, President, Railway Supply Institute .....	6
Prepared statement .....	32
Responses to written questions of:	
Senator Cotton .....	56
Scott N. Paul, President, Alliance for American Manufacturing .....	8
Prepared statement .....	37
Responses to written questions of:	
Senator Cotton .....	57
Senator Warren .....	62
Emily de La Bruyere, Principal, Horizon Advisory .....	10
Prepared statement .....	44
Responses to written questions of:	
Senator Cotton .....	64
Frank J. Cilluffo, Director, McCrary Institute for Cyber and Critical Infra- structure Security, and Director, Center for Cyber and Homeland Security, Auburn University .....	13
Prepared statement .....	50
Responses to written questions of:	
Senator Cotton .....	66
Senator Warren .....	69
Senator Sinema .....	71

## ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Statement from Portland Cement Association .....	72
Letter from Rail Security Alliance .....	74
Letter from Securing America's Future Energy .....	76
Letter from VIA Metropolitan Transit .....	78



## **THREATS POSED BY STATE-OWNED AND STATE-SUPPORTED ENTERPRISES TO PUBLIC TRANSPORTATION**

**THURSDAY, MARCH 5, 2020**

U.S. SENATE,  
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,  
*Washington, DC.*

The Committee met at 10:03 a.m., in room SD-538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

### **OPENING STATEMENT OF CHAIRMAN MIKE CRAPO**

Chairman CRAPO. The Committee will now come to order.

Today's hearing will focus on the threats posed by State-owned and State-supported enterprises on public transportation.

Last year, Ranking Member Brown and I were original cosponsors with Senators Cornyn and Baldwin in introducing S. 846, the Transit Infrastructure Vehicle Security Act, language that served as the basis for Section 7613 of the National Defense Authorization Act, or NDAA, which was enacted in December.

As you will see today, this issue has broad bipartisan support.

There are 52 bipartisan cosponsors of S. 846, and more than half of the Members of this Committee, on both sides of the dais, are among that list.

The provisions in S. 846 are also supported by the Trump administration, both in a Statement of Administration Policy regarding the House NDAA and Acting OMB Director Russell Vought's letter to the House and Senate Armed Services Committees supporting the language ultimately reflected in Section 7613.

Today's expert witness panel reflects the multifaceted nature of threats BYD and CRRC pose to our national security, the economic competitiveness of the domestic bus and rail manufacturing industry, and cybersecurity.

All of the witnesses have been valuable resources to the Committee as we got the language of S. 846 enacted into law, and we thank them for their expertise and willingness to help.

From a national security perspective, 15 former generals and admirals from the Energy Security Leadership Council wrote a letter warning of the Chinese strategy to dominate critical industries.

The former military leaders stated that the "Chinese industry is inexorably intertwined with Chinese Government, which creates a host of economic and national security concerns for the United States."

Economically, both CRRC and BYD include direct subsidies from the Chinese Government in their annual reports.

There are presently at least seven other transit railcar manufacturers besides CRRC and at least five other transit bus manufacturers besides BYD in the United States.

It is impossible for other bus and rail manufacturers to fairly compete when these two companies have the unfair advantage of the financial support of the Chinese Government.

As transit agencies are working to address the \$98.8 billion state of good repair backlog in the industry, they are often looking to modernize, such as transitioning to electric buses and incorporating autonomous technologies.

Along with the modernization comes increased connectivity, which increases the threat of cyberincidents and espionage.

The language enacted in Section 7613 of the NDAA acknowledges that all of these threats are real and applies significant new restrictions on funding for the acquisition of CRRC railcars and BYD buses.

It is unfortunate that Section 7613 includes a 2-year delay on the prohibition, and it is critical that transit agencies immediately understand the threats associated with purchasing from a State-owned or State-supported entity and how that should affect their procurement decisions now and looking ahead.

Recently, Senator Brown and I, along with House Transportation and Infrastructure Chairman DeFazio and Ranking Member Graves, wrote to Secretary Chao emphasizing the urgent need for the Department of Transportation to put out information online or issue a “Dear Colleague” so that transit agencies are informed of the new law and can plan their rolling stock procurements accordingly.

We have already heard anecdotally that both BYD and CRRC have been seeking to misinform agencies as to the applicability of the language.

In order for agencies to make informed procurement decisions, it is critical that the Administration respond and give transit agencies the tools they need to understand how to comply with the statute.

Senator Brown.

#### **OPENING STATEMENT OF SENATOR SHERROD BROWN**

Senator BROWN. Thank you, Mr. Chairman, for calling today’s hearing on the bipartisan bill. I appreciate our friend Senator Baldwin being here. Thank you. And Senator Cornyn I believe was called away at the last minute, but thank you for your work, Tammy.

Senator Baldwin and Senator Cornyn have been partners in our Transit Infrastructure Vehicle Security Act. Members of this Committee also supported and cosponsored the bill. Thank you to them.

Our Committee’s bipartisan work to address a threat to public transportation from companies supported and controlled by the Chinese Government shows that our Government can be nimble in responding to new economic and security threats. We must be vigilant. It is why just this week Senators Baldwin and Cornyn and

Crapo and I have sponsored an amendment to the energy bill on these issues.

While TIVSA is now law, we need to keep our focus on the two Chinese companies in question: CRRC and BYD. These companies have repeatedly shown that they do not play by the rules.

Let us talk first about CRRC. As a State-owned enterprise, they did not have to worry about making a profit when it used low-ball bids to win four major U.S. contracts for transit railcars.

In 2014, CRRC offered a bid on the Boston MBTA contract that was more than \$150 million lower than the next competitor. In Chicago in 2016, they beat the next lowest bidder by \$226 million.

That is not because they were doing the work more efficiently. It is because they were subsidized, propped up by the Chinese Government. So it is not surprising that established manufacturers were simply unable to match these bids.

That is not the full picture, though, of the damage from CRRC's low-ball bids.

Hyundai-Rotem manufactured railcars for Philadelphia's SEPTA system and Denver's RTD system. The 300 Hyundai workers in its Philadelphia factory were represented by Transport Workers Union, TWU, Local 234. They made a middle-class living wage with employer-provided benefits and a retirement plan. All of these workers lost their jobs after Hyundai-Rotem lost the SEPTA contract to CRRC.

Hyundai closed the plant in August of 2018. For every U.S. job created by CRRC, it is estimated the U.S. loses between three and five jobs.

Before Congress acted last year, CRRC was making plans to win a contract with the Washington, D.C., Metro worth more than \$1 billion.

And then there is the electric bus maker BYD, another company covered by TIVSA. I want to be clear: My concern with CRRC and BYD is not with the American workers they employ, but with the Chinese Government's influence and control.

I spoke last night with Senator Cortez Masto discussing the transportation union SMART. We will always stand with our union brothers and sisters. That is not the issue here. To me, it is about workers. To most of us, it is about the workers. But our concern is with the Chinese Government's influence and control.

BYD may not be technically owned by the Chinese Government, but it is certainly controlled by it. As our expert witnesses will testify, BYD may receive even more State support than CRRC, and BYD has deep ties to the Chinese Government.

BYD's goals in the U.S. extend far beyond the public transportation system. It supplies electric trucks for freight delivery; it offers electric garbage trucks to cities; it is eyeing the passenger car market.

There are four other major bus manufacturers that build electric buses in the U.S.; two are American-owned. These companies are ramping up their production of zero-emission buses to help American transit agencies reduce emissions, but they do not enjoy enormous support from the Chinese Communist Party.

This is an industry of the future. It is more and more important in our economy. It is more and more important to deal with the science of climate change. We cannot cede it to China.

BYD likes to point out that Warren Buffet is an investor in their company. One billionaire investor does not mean that BYD is looking out for the interests of American workers.

CRRC and BYD are two in a long line of examples of how China cheats its way—many in this audience, I know several of you have been part of this struggle for decades—how they cheat their way into being a global leader in industry after industry after industry. Ohio's steel industry knows that too well.

For years, Chinese State-owned steel companies have been flooding our markets and the global markets, forcing steelworkers in my State out of their jobs.

It is why we have taken more than 60 trade enforcement actions against Chinese steel producers, to help create a level playing field for American producers.

CRRC and BYD, though, undermine those trade enforcement efforts by purchasing Chinese steel, turning it into frames and shells for buses and railcars at factories in China, then shipping them to the U.S. for final assembly, and they get bought using U.S. tax dollars, threatening steelworker jobs.

It is exactly the kind of cheating you would expect from sophisticated Chinese companies that refuse to play by the rules.

It is a jobs issue, and it is a national security issue.

When we let Chinese companies manufacture our buses and railcars, we face cyber and data security risks. Our hearing today will discuss these concerns facing transit agencies and our broader transportation sector. TIVSA created an important new requirement for transit agencies to assess cybersecurity risks, but Congress still needs to fully assess the risks associated with data from our transportation system being exposed to foreign actors.

We know the threat of Chinese State-owned enterprises investing in the U.S. is not limited to rail and bus manufacturers. We do not even know all the ways in which companies owned or controlled by the Chinese Government are gaining footholds in our market.

My legislation with Senator Grassley, the Foreign Investment Review Act, would require the Secretary of Commerce to review certain foreign investments, particularly those made by State-owned enterprises, to make sure they are in the long-term, strategic interests of American workers and American businesses. This is an example of bipartisan legislation that actually can help address new economic and security threats.

I will close by noting that as we work to reauthorize transit programs—and I look at Senator Baldwin's leadership particularly—we need to strengthen Buy America requirements. It is not complicated. American tax dollars, shockingly, should support American jobs.

Thanks.

Chairman CRAPO. Thank you, Senator Brown.

We have two panels today. Senators Cornyn and Baldwin will be our first panel. As you can see, Senator Cornyn is not here. He has been called away. We do not know if he will make it back. If he does get back later, we may interrupt the second panel to allow



him to make his statement. But we do have Senator Baldwin here, and we appreciate you being here, Senator Baldwin. You may proceed.

**STATEMENT OF SENATOR TAMMY BALDWIN OF WISCONSIN**

Senator BALDWIN. Thank you. Thank you, Chairman Crapo and Ranking Member Brown. I am delighted to have the opportunity to be here today to discuss our legislation, the Transit Infrastructure Vehicle Security Act, which became law in December 2019 as part of the National Defense Authorization Act for Fiscal Year 2020.

This law is important to me in short because Wisconsin is a State that makes things. For generations, we have assembled our Nation's ships, built our Nation's engines, and brewed our Nation's beer. However, since we allowed China to enter the World Trade Organization in 2001—a move I opposed—millions of manufacturing jobs have been lost. And many workers have seen their wages stagnate as a result of downward pressure from competition from Chinese State-backed companies.

As a nonmarket economy, China gives hundreds of billions in State subsidies to manufacturers in industries in which the Government wants to compete. In 2015, the Chinese Communist Party released a strategic document outlining how it intends to compete globally in manufacturing. It was called “Made in China 2025”.

This plan revealed that China desires to dominate in railcar and electric bus manufacturing. Recently, two State-supported companies have made inroads into the U.S. market: the railcar manufacturer China Railway Rolling Stock Corporation, which we refer to as CRRC, and the bus and electric battery manufacturer Build Your Dreams, which we refer to as BYD.

We know from observing CRRC's entry into the Australian market that domestic industry cannot compete with China's aggressive State-owned enterprises. Over the last 15 years, Australia's domestic railcar production collapsed as CRRC gained increasing market share.

Wisconsin manufacturers are happy to compete with anyone in the world, but we need a level playing field. And China's non-market economy forces Wisconsin manufacturers to compete with Chinese companies that get free land, free utilities, free R&D, and interest-free loans worth hundreds of millions of dollars.

These Chinese Government-subsidized rivals would be bad enough, but now these companies are increasingly using their U.S. assembly facilities to win taxpayer-funded contracts from the Federal Transit Administration to procure buses and railcars for American cities.

When taxpayer dollars are spent, I believe we must make every effort to ensure that they support American workers and businesses. As a strong supporter of expanding and improving Buy America policies, I was proud to join Senators Crapo, Brown, and Cornyn in introducing and passing legislation to prohibit FTA funds from going to companies supported by nonmarket economies, such as BYD and CRRC.

In 2 years, the prohibition in that law will go into force. Transit agencies need to know how they will be affected as soon as possible. Senator Cornyn and I have both requested that Secretary

Chao and Acting FTA Administrator Williams publish information to ensure that transit agencies planning for the future are able to make safe, informed, and legal procurement decisions.

While the legislation addressed many immediate concerns facing the domestic railcar and bus manufacturing industries, I urge this Committee to work with the Department of Transportation to further tighten Buy America requirements to ensure that Federal taxpayer dollars support good-paying manufacturing jobs in the U.S.

I am deeply concerned by a study from *Oxford Economics* that found that CRRC's railcar production in the U.S., while compliant with Buy America, relies heavily on imported parts. This particular report estimated that, as a result of this "import and assemble" business model, every one job CRRC creates in the U.S. eliminates as many as five U.S. jobs.

I will close by commending the Committee on the oversight work it is doing to ensure that this law is implemented as swiftly and as effectively as possible and once again thank you the Chair and Ranking Member for the opportunity to testify here today.

Chairman CRAPO. Thank you, Senator Baldwin. We appreciate your work on this issue, and we will continue to work with you to make sure that these policies are implemented effectively. Thank you.

Senator Cornyn has not yet arrived, so we will now move to our second panel. Would the panelists please come forward?

[Pause.]

Chairman CRAPO. Thank you. And on our second panel, we will receive testimony from Mr. Michael O'Malley, president of the Railway Supply Institute; Mr. Scott Paul, president of the Alliance for American Manufacturing; Ms. Emily de La Bruyere—did I pronounce that right?—principal of Horizon Advisory; and Mr. Frank Cilluffo, director of the McCrary Institute for Cyber and Critical Infrastructure Security and director of the Center for Cyber and Homeland Security at Auburn University.

You may all proceed. We ask you to stick to your 5 minutes so that we can get our questions in. And, again, we welcome you here and appreciate the work that you have already put in and the assistance you have already given and your willingness to help us here today.

Mr. O'Malley, you may begin.

#### **STATEMENT OF E. MICHAEL O'MALLEY, PRESIDENT, RAILWAY SUPPLY INSTITUTE**

Mr. O'MALLEY. Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you very much for the opportunity to testify today on threats facing public transportation systems from foreign State-owned and State-supported enterprises, an issue that is of critical importance to the railway supply industry and the Nation. My name is Mike O'Malley, and I serve as president of the Railway Supply Institute, an international trade association representing more than 200 companies who manufacture or deliver goods and services in the locomotive, freight railcar, maintenance of way, communications and signaling, and passenger rail industries.

The rail system of the United States is one of our country's greatest assets, covering more than 140,000 miles and carrying 40 percent of America's intercity freight, including 111 million tons of hazardous materials, each year. It also transports millions of passengers every day, from small transit systems to large commuter authorities to intercity service provided by Amtrak or other entities. These systems are supported by an extensive domestic railway supply industry that has been a dynamic and vital part of the U.S. economy for over 200 years, encompassing 125,000 jobs across all 50 States and paying an average wage 40 percent above the national average. Without this industry, our Nation's passenger and freight railroads simply could not meet their customers' critical needs.

Unfortunately, over the past decade our industry has witnessed substantial intervention in the global rail marketplace from non-market economy foreign Governments. Most notably, the People's Republic of China—working through State-owned enterprises like CRRC—has identified rail manufacturing as a strategic market sector and made clear their intention to, in their words, “conquer” the global rail market. As a State-owned enterprise, CRRC benefits from the full resources of the Chinese Government and has been repeatedly used to spearhead strategic initiatives identified by the Chinese Communist Party. Backed by these virtually unlimited resources, CRRC and its affiliates have leveraged direct subsidies, State-backed financing, and below-market loans to secure more than \$2.6 billion in railcar contracts at far below market rate for transit agencies in Boston, Chicago, Los Angeles, and Philadelphia. These contract awards present both economic and national security risks. As many national security experts have pointed out, China has demonstrated that the technologies on railcars can be used for illicit means.

On the economic front, CRRC's anticompetitive practices are threatening thousands of high-paying man jobs and putting the long-term future of this industry at risk. We have seen what can happen when CRRC is left to continue these practices unchecked.

In Australia, Chinese State-owned enterprises decimated the rolling stock market in less than 10 years, leaving CRRC as effectively the sole supplier of both freight and passenger railcars. Rail manufacturers want a free and fair global market that promotes competition, but they should not be expected to compete against the unlimited resources of a foreign Government.

The rail manufacturing industry is grateful for the actions policymakers have taken thus far to mitigate CRRC's threat, whether through much needed reforms to the Committee on Foreign Investment in the United States or the more recent passage of the Transit Infrastructure Vehicle Security Act as part of the 2019 national defense bill. These legislative achievements are important steps forward, but the threat remains.

Looking ahead, I would offer the following recommendations for policymakers to continue being proactive in countering this threat: First, the Federal Transit Administration should immediately communicate with its grantees the restrictions contained in the TIVSA bill to ensure compliance with this new law.

Second, Congress should pass a long-term infrastructure bill with robust passenger rail funding levels to ensure that States and localities can make smart, sustainable investments for the future.

Third, the U.S. Department of Transportation should be given additional resources to ensure strict, consistent compliance with Buy America rules, supporting domestic jobs and preventing foreign State-owned enterprises from gaming the system.

And, finally, Congress should pass legislation to create safeguards for the freight rail industry as well.

Given the global nature of this threat, many of our allies are now following the lead of U.S. policymakers to address this issue. RSI members will continue doing all we can to support our passenger agency customers in serving the mobility and economic development needs of communities across the country, but we cannot be expected to compete in a marketplace that is distorted by Chinese Government subsidies and intervention.

We appreciate the opportunity to provide these recommendations and will continue working with Members of Congress to formulate policies that enhance rail safety, security, and efficiency. Thank you very much for the opportunity to testify, and I will be happy to answer any questions you may have.

Chairman CRAPO. Thank you very much.

Mr. Paul.

#### **STATEMENT OF SCOTT N. PAUL, PRESIDENT, ALLIANCE FOR AMERICAN MANUFACTURING**

Mr. PAUL. Thank you, Chairman Crapo, Ranking Member Brown, and Members of the Committee. On behalf of the Alliance for American Manufacturing, I want to thank you for the opportunity to testify.

AAM is a partnership between the United Steelworkers Union, which is America's largest industrial union, and some leading American manufacturers, and together we have seen the destructive impacts of China's model of State-led capitalism on our domestic manufacturing sector and the damaging ripple effects on thousands of communities across our Nation. Between 2001, when China entered the WTO, and 2018, 3.7 million U.S. jobs were lost or displaced because of the massive bilateral trade deficit with China. This carnage has been fueled by predatory trade practices and disruptive economic policies, including massive subsidization of State-owned enterprises and other "champion" firms that Beijing has deemed strategically important to their own economic and security interests.

More recently, we have witnessed China's State-owned and State-supported rolling stock companies threaten legitimate competition in the markets that serve our public transportation system. Backed by extensive Government support, including Made in China 2025, CRRC and BYD are at the forefront of China's assault. Their penetration into our market has been accelerated by open access to taxpayer-financed railcar and electric bus procurements in major U.S. cities. In other words, these firms have penetrated our market not only with Beijing's backing, but also on the backs of American taxpayers.

China's subsidies and other governmental support allow CRRC and BYD to underbid the competition. Left unchecked, the toll on U.S. supply chains will be devastating. Because CRRC and BYD's U.S. assembly operations are a supply line for major rolling stock components produced in China, the jobs of American workers throughout our domestic supply chains are now at risk. CRRC's train shells are made with Chinese metals and assembled with substantial Chinese parts in their stateside operations. Meanwhile, a city official familiar with BYD's assembly operations remarked that, "the majority, if not all, parts were manufactured in China and shipped to the United States."

China's ambitions are sizable: to establish a substantial foothold into our public transit market as a means of expanding into private sectors such as the freight rail and electric vehicle markets. Jobs, supply chains, innovation, and the security of Americans using our public transportation systems are all at risk. We are also deeply concerned about China's "military-civil fusion" partnerships. Put simply, technology and data obtained by these firms in the United States is handed directly to the Chinese military, and each collaborates with Huawei.

We are grateful that Congress, under your bipartisan leadership, has begun taking action to mitigate this threat. Your bipartisan leadership led to passage of a version of TIVSA as part of the fiscal year 2020 NDAA. If TIVSA is properly implemented as intended by Congress, CRRC and BYD will no longer have unfettered access to our Federal tax dollars used to procure public transit vehicles. The TIVSA law represents an important milestone in the U.S. policy response to the threat of China's State-driven gaming of our economy.

But already there are forces at work to undermine TIVSA. Shortly after enactment, CRRC held a "thank you" event at which speakers discussed plans to indefinitely extend the 2-year implementation delay. And in Los Angeles, BYD recently secured a bus order for 135 buses. So we urge Congress to reject any attempts to undermine the TIVSA law. Instead, AAM supports efforts to accelerate implementation, educate transit agencies, and enhance the law.

First, we must ensure the Administration implements the TIVSA law without delay and as Congress intended and reject short-sighted attempts to undermine the law.

Second, we must be better stewards of U.S. tax dollars by closing loopholes by strengthening and by ensuring compliance with applicable Buy America laws.

And, finally, we must incentivize the production of electric vehicle batteries and battery cells in the United States and invest in America's failing infrastructure.

Again, thank you for the opportunity to testify at today's hearing. My full testimony has detailed information on CRRC and BYD along with detailed policy commission. We look forward to working with you.

Chairman CRAPO. Thank you very much.  
You may proceed, Ms. de La Bruyere.

**STATEMENT OF EMILY DE LA BRUYERE, PRINCIPAL, HORIZON  
ADVISORY**

Ms. DE LA BRUYERE. Thank you, Chairman Crapo, Ranking Member Brown, for the opportunity to testify.

I am here to tell you about Beijing's plan, about the strategic vision with which it deploys its State champions internationally and about the implications of that vision for American security.

CRRC, BYD, and the larger ecosystem of Chinese champions in transportation, but more broadly across foundational ecosystems, operationalize a longstanding, documented bid to overtake the United States. That bid begins by making critical U.S. economic and military systems dependent on China. It ends with a world in which Chinese Communist Party control over global networks, standards, and platforms grants them control over global movement. This is network hegemony.

China's ambition is evident in authoritative strategic discourse. It is equally evident in the facts: in the subsidies, in the mandates assigned State champions, in the industrial and strategic planning underlying all of this. That planning includes Made in China 2025. It also includes China Standards 2035. It includes the Strategic Emerging Industries Initiative, but it also includes the Transportation Great Power Strategy.

I would like to emphasize at the outset that BYD and CRRC are critical, but they are just the tip of the iceberg. As I speak, any number of other Chinese State champions are integrating themselves into our foundational systems, both so that we depend on them and so that we fuel them. They are not just doing so in rail and road, but across the entire transportation and logistics ecosystem, not just in transportation and logistics but across FinTech and social media, in surveillance and sensors, across the bio-economy, space, the Internet of Things. But for today, BYD and CRRC first.

CRRC is a State-owned enterprise. BYD is a private company. Both receive hundreds of millions of U.S. dollars' worth of Chinese Government subsidies every year, which is orders of magnitude more than they report in their English language annual statements.

In BYD's case, its subsidies exceed its operating profit. These subsidies stem for Chinese industrial planning that is designed to prop up the transportation sector, writ large, so that Chinese champions can dominate global markets, but also so they will do so according to Chinese Communist Party guidance. This mandate is codified in Xi Jinping's Transportation Great Power Strategy. That strategy was issued in October 2019 as this body was debating TIVSA.

The strategy lays out China's plan to export a global transportation network. It will connect highways, railways, waterways, aviation, pipelines, postal services, freight. It is to be built by Chinese champions on Chinese information systems to export Chinese standards. It is to connect back to a Beijing-controlled big data repository. It will also connect to BeiDou's space network and to Huawei's telecommunications network. For the record, BYD and CRRC cooperate with both of those companies.

China's vision is not rhetoric and it is no distant future. The Transportation Great Power Strategy lays out a plan for a multi-dimensional logistics information network. This network is in place. No one is talking about it. It connects the global infrastructures in which China invests to a domestic data hub and information system. Beijing has secured the support of ASEAN's NEAL-NET and Europe's IPCSA so that they proliferate China's coercive tool. Ostensibly private companies also partner with this system so that it can extend its net more broadly and more subversively. That there is a key part of the Transportation Great Power Strategy. It is explicit about the fact that this network will extend internationally, fueled by foreign investment and thanks to partnerships among international actors and Chinese companies. BYD and CRRC have explicitly labeled themselves as champions of the Transportation Great Power Strategy, and all of this is part and parcel of the military-civil fusion program.

BYD, CRRC, Huawei, and BeiDou, the larger litany of ostensibly civilian champion, operate in conjunction with Beijing's military system, with joint ventures, with research partnerships, with domestic and international investment vehicles. These partnerships are designed to transfer technology and data seamlessly between the military and the civilian. More broadly, they are designed to transform the commercial field into a geopolitical battleground. This adds up to an entirely new form of power projection, one in which China not only has coercive but also has shaping power. Recent jamming events at the port of Shanghai hammer this home in the military domain. China's corporate social credit system does the same economically. But China is proliferating its web through commercial—through civilian actors, not through explicitly military tools. That means we miss what they are doing. We also risk fueling it. We should not be giving Federal funding to China's champions.

Chairman Crapo, Ranking Member Brown, thank you for this opportunity. I look forward to your questions.

Chairman CRAPO. Thank you very much.

We have been joined by Senator Cornyn now. Mr. O'Malley has graciously let him take his seat for his testimony. He says he is happy to do it.

Senator Cornyn, we welcome you and we open the floor to you. You may make your statement.

#### **STATEMENT OF SENATOR JOHN CORNYN OF TEXAS**

Senator CORNYN. Well, thank you Mr. Chairman and Ranking Member Brown, Senator McSally, and Members of the Committee. Thank you for inviting me to share my thoughts with you on this topic. This is important to my State and your State, our national security, and the integrity of our entire economy.

China has, of course, a long history of undermining market economies across the globe by subsidizing Chinese businesses so they can outcompete domestic industry, because they never have to worry about turning a profit.

Global domination of rolling stock production, like trains and buses, is at the forefront of the Made in China 2025 initiative,

which outlines the Chinese Communist Party's plans for economic domination across the globe.

That is why I was concerned when I found out certain Chinese State-controlled companies like the China Railway Rolling Stock Corporation and Build Your Dreams were submitting unrealistically low bids for transit projects in major U.S. cities in an attempt to put competition out of business and dominate the market on a long-term basis.

Transit railcars and buses are highly advanced vehicles. They are equipped with a host of computers, sensors, and cameras.

When an American steps into a subway or city bus, they accept that many of these devices are there to ensure their safety and trust that the Government will not use them to abuse their civil rights.

But these advanced technologies can do much more than help you get to work on time. They are also capable of spying on passengers and our infrastructure network, and they can be undetectably placed on transportation systems across America.

Thousands of Government and military officials use transit services every day, especially here in the Nation's capital. I am sure many of the folks in this room relied on those transportation facilities to get here today.

The potential for an adversarial State actor to monitor the movement of American citizens, hack personal or Government-issued devices, and collect intelligence on our military is a major security concern.

Allowing American trains and buses to become Trojan horses for these technologies on American soil is simply unacceptable.

And I think we can all agree that Chinese State-controlled companies should not receive a dime of American taxpayer money in their efforts to control our economy and undermine national security.

Fortunately, Congress has taken an important step to address that problem.

Senator Baldwin, the Chairman, and Ranking Member have joined us in getting the Transit

Infrastructure Vehicle Security Act passed into law as part of the National Defense Authorization Act last year.

This commonsense, bipartisan legislation sends a strong signal to the Chinese Government that we will not allow them to infiltrate the operations of our critical infrastructure.

The legislation will ban the use of Federal transit funding for the procurement of railcars and buses produced by companies that are owned, controlled, or sponsored by foreign Governments with non-market economies and that are designated as countries of concern by the U.S. Trade Representative.

Unfortunately, special interests were able to demand a 2-year enforcement delay of some of this legislation's critical components.

I am here today to ask for your help in ensuring this delay does not turn into a window of opportunity for the Chinese Communist Party and its State-controlled companies to further exploit our vulnerabilities here by rushing to procure contracts and extending their tentacles further into America's infrastructure network.



Without strong leadership from the Federal Transit Administration, transit agencies will unknowingly allow CRRC and BYD to compete for their projects, even though a Federal ban on those contracts is just around the corner. We have to do everything we can to stop it in the interim.

I look forward to working with you, Mr. Chairman, the Ranking Member, and other Members of this Committee to help educate U.S. Government agencies, the public, and our local jurisdictions about China's threat to our infrastructure, and the legal tools Congress has enacted to address this problem.

Thank you for the opportunity to speak to you today, and thanks for accommodating my schedule.

Chairman CRAPO. Thank you, Senator. We are glad you were able to get here, and we appreciate not only your testimony today but your work on this issue. We look forward to continuing to work with you, and the message you suggested needed to be sent is one of the purposes of this hearing. You may be excused, and you can let Mr. O'Malley have his seat back. Thank you.

And we will proceed to Mr. Cilluffo.

**STATEMENT OF FRANK J. CILLUFFO, DIRECTOR, MCCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY, AND DIRECTOR, CENTER FOR CYBER AND HOMELAND SECURITY, AUBURN UNIVERSITY**

Mr. CILLUFFO. Thank you, sir.

Chairman Crapo, Ranking Member Brown, thank you for the opportunity to testify before you today and thank you for your leadership and that of your colleagues, such as Senators Cornyn and Baldwin, in getting the ball rolling legislatively in this important subject area.

I do not think I have ever testified at a hearing where I agree with every opening statement from everyone here. So rather than try to go deep in a whole bunch of areas, I will double tap a couple of points and foot stomp a couple of points. But quite honestly, the hearing—the statements have been excellent and I agree with almost every single point.

So this hearing speaks specifically to the threat posed to public transportation by State-owned and supported enterprise. On this question, as everyone said, I will speak very plainly. The chief threat comes from China and certainly includes the sale and provision of railway cars to U.S. transit systems. But the threat also extends far beyond that to all critical infrastructure, as Ms. de La Bruyere had mentioned.

And here is how it works. As others have made loud and clear, a nonmarket economy can underbid U.S. firms. And it is about more than simply an unlevel playing field. A foothold in the U.S. supply chain gives rise to a host of concerning possibilities ranging from computer network exploit or espionage, mapping of our critical infrastructure, or intelligence preparation of battlefields, and/or computer network attack, disruptive or destructive attacks.

I want to underscore here that if you can exploit, you can also attack if the intent exists to do so.

Companies may be willingly or even unwittingly serve as conduits of sensitive information as Chinese legal provisions allow

their security services to request and even compel assistance. Even worse, China's challenge is not just economic. It is part of this broader strategy that others have discussed on strategic dominance.

And apropos to this Committee, a majority of the critical technologies targeted by the State Council's Made in China 2025 are directly or indirectly related to the transportation sector. And I can say the same with some of the other roadmaps, notably on space.

With respect to transportation specifically, here is the problem: the potential for continuous and direct access to our railcar and transit systems is real. The consequences, an adversary could shut down trains and disrupt operations. Knock-on effects could hit other critical U.S. infrastructure and major U.S. cities could experience significant economic effects.

The bottom line, U.S. national and economic security are inextricably interwoven and we need to work harder to inoculate ourselves and better manage the risk. Consider the scale and scope. FBI has about 1,000 investigations in all 56 field offices, spanning just about every industry and sector, all related to China. U.S. companies and U.S. universities are both targets all over the country from Alabama to Iowa. Plus, China plans to double its current research spending to reach over \$800 million for recruitment via its Thousand Talents Program, as the National Intelligence Council recently released. And that includes the buyout of bankrupt companies, which I think is a big set of issues to acquire technology.

Our current and future ecosystem is replete with risk, especially as the attack surface grows exponentially. Whatever we do, we cannot afford to build advanced systems like 5G and IoT on quicksand. The potential to do so is, unfortunately, real.

Also, keep in mind that the transportation sector supports and intersects with other critical missions, infrastructure, and functions. For example, defense mission assurance, the ability to project power and deploy forces and the link between rail system switches and positioning, navigation and timing or PNT. Think GPS, think timing and signaling. And no surprise, China has also invested heavily in its space programs, to include antisatellite capabilities.

So what to do? Very quickly, third-party testing. Kudos to your legislation. I think the provisions on cybersecurity certification ought to serve as a model for other critical infrastructures. Incentive security, leverage the market forces. Action will entail costs, but inaction will be much more costly.

Start with the lifeline sectors, the most critical of our critical infrastructures. Identify, assess and manage risk continuously. This cannot be a reactive, check-the-box exercise. Scrutinize our supply chains, use systems of systems thinking. On the technology side, I would urge a nationwide R&D test bed-type network. You need not look further than the recent coronavirus crisis to realize how important, from an economic perspective, our supply chains are. Obviously, the public health issue is number one, but the economic implications are striking, as well.

Integrate cyberfactors writ large and elevate corporate governance. So this is not just the IT guy or gal's job. This is a corporate governance set of issues and we need to build in rigor with empirical data into policymaking.

And then finally, because I know I am over my time, more human capital—the workforce challenges here are immense—and resources. We do now have an opportunity to lash up the arms and the legs of Government, notably NSA, DOD, DHS CISA, and the Department of Transportation.

I thank you for the opportunity to testify. I am sorry, I did not make it on time.

Chairman CRAPO. That is all right.

I am going to ask the first question to each of you, and I have 5 minutes, so I will ask you to each try to take about a minute in responding to this.

We find ourselves in a very connected world. It seems like everything we have now is a smart device. I would like you to talk for a second about what type of smart capabilities are now or could be developed to be utilized in our transit system infrastructure? And maybe some of the ways or risks that this generates in terms of the risk of vulnerability to attack or hacking or monitoring or even more malign purposes.

So if you would, let us just start over with you, Mr. O'Malley. And if you could each try to keep it to about a minute, I would appreciate it.

Mr. O'MALLEY. Absolutely. I think what I would say, from our perspective as rail manufacturers, there are a whole host of technologies that are being used, both in the transit side of the business as on the freight side. And that is everything from advanced train control technologies like PTC to better use of GPS and Wi-Fi and surveillance technologies, if you will, making sure that the systems are running more efficiently.

I think those are helpful things, in many ways, but they also carry risk in terms of the way they can be used. And I think the challenge here is inserting a Chinese State-owned enterprise into the middle of all of that risk and not knowing sort of what their motivations are and how they might act in that respect.

Chairman CRAPO. Thank you. Mr. Paul.

Mr. PAUL. I will make two brief points. First, is that CRRC and BYD, if there are concerns about the types of data that are being collected, it is easy to secure either subpoenas or other sorts of legal actions to compel American-based firms to supply that. For firms that are based in China, it is extraordinarily difficult to do that. And CRRC and BYD both ultimately answer to Beijing. That is number one.

Number two, in a hearing on the House side, and I think this is a very important point, with the advent of facial recognition technology and the fact that all of this equipment has video surveillance monitors—some for good reason—it presents the very real possibility the Chinese Government could access this not only to spy on us but also their dissidents, as well, who have sought refuge in the United States against the oppressive regime. I am incredibly concerned about that.

Chairman CRAPO. Thank you. Ms. de la Bruyere.

Ms. DE LA BRUYERE. So those first order security threats are very real. But there is also the potential for strategic information advantage and information shaping that comes from controlling these keystone positions in an interconnected world. So first, infor-

mation dominance. If Beijing has these railcars, it knows—because they are connected—with better information, how resources are moving around in the U.S. That gives it an inherent market advantage because that is the kind of information that shapes how markets are going to work. That market advantage extends to all sorts of other domains and it also works in the political, the strategic, the kinetic domain.

Then there is the shaping. If these information systems are controlled by Beijing, it can shape the information they disseminate. So these cars, these rails, these buses, they are going to turn into autonomous driving systems. So that means that China has a hand in determining the—no longer GPS where the BeiDou behind that autonomous system is telling you to go in your path. Or what the media that is playing in the car when you walk in in the morning is. And so that creates a world that is operating according to Chinese rules where they dominate the narrative that is being disseminated, the choices that are being made, the incentives more broadly.

Chairman CRAPO. Thank you. Mr. Cilluffo.

Mr. CILLUFFO. Mr. Chairman, thank you.

That is an excellent question because I may have been a little dramatic saying we do not want to build our systems on quicksand. But the reality is that that is potentially where we are going if we do not take a systems of systems approach here.

It is much cheaper, smarter and better to bake security into the design of our infrastructures than try to bolt it on after the fact. And I think transportation—I mean, when I think of autonomous vehicles, the highways of tomorrow are going to be paved in silicon as much as they are in asphalt. It is all going smart, which has great opportunity but it does bring about peril and risk.

That is why the core operating systems, the foundations upon which all these systems are built, we do not want to hand that over to anyone but U.S. companies. I think China, as Mark Twain said, history may not repeat itself, but it tends to rhyme. If you have looked at the historical role that China has played in intellectual property theft, it should be loud and clear how we need to be going toward that.

But in addition to intellectual property theft, if you are in the core of the system, you can disrupt and/or turn toward destructive attacks. And U.S. DOD is dependant upon civilian infrastructure to be able to deploy forces. Imagine if you stymied the ability to be able to deploy or project power.

So there are a number of national security issues here. But I would just say when you look at 5G, Huawei, these are the hubs and spokes sorts of issues we need, as a country, to get right or we will be paying a big, big, big price long-term.

Chairman CRAPO. Thank you.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

My first question is for Mr. O'Malley and Mr. Paul, if you would each answer it. As Chairman Crapo noted, we joined with Chairman DeFazio and Ranking Member Graves of the House Transportation and Infrastructure Committee in sending a letter to DOT asking Secretary Chao to immediately provide information to

grantees about the TIVSA provision so that U.S. transit agencies can be fully aware of the new restrictions on procurement and so there is no misinformation in the market. We sent our letter January 31st, DOT has not taken action.

Mr. O'Malley, are you aware of any reason they could not quickly distribute information in a letter or on its website? Is there any reason or, maybe better yet, excuse for this delay?

Mr. O'MALLEY. No, we are not aware of any reason why they cannot. And frankly, we share your concerns and we would like to see them communicate immediately with their grantees.

You know, the will of Congress, I think, is very clear here. We were disappointed with the 2-year delay, as you all were, as well. But this is a national security threat and I think we have to act in that fashion and quickly.

Senator BROWN. Mr. Paul.

Mr. PAUL. I completely agree with Mr. O'Malley. There is no plausible reason why at least initial guidance could not have been provided by now, particularly since this provision was put into place as part of the NDAA bill and is viewed with some national security implications and WMATA specifically was excluded from procurement possibilities for CRRC. There is a recognition that there is a security imperative to this.

So it is not merely a procurement guideline and I wish every agency would take it more seriously than it has so far.

Senator BROWN. Yes, we cannot really figure it out either, Mr. Paul.

Just for you, today's hearing offers clear evidence that China's State-owned steel companies and China's transit manufacturers hurt U.S. companies and manufacturers are undermined by America's standards. Not every infrastructure program, as you know, is covered by Buy America which means taxpayer dollars can still be spent on steel from China or anywhere else.

Do you believe our piecemeal approach to Buy American adequately protects American taxpayers from subsidizing Chinese steel companies or other foreign-based manufacturers? And is there any reason we should not apply Buy America policies that we have in the transit space to all Federal infrastructure?

Mr. PAUL. Yes, Senator Brown, that is an excellent question and I completely agree with you. I know that you and others have introduced legislation for a broader application of domestic preferences and Buy America laws, in particular.

We think that there are tens of billions of dollars in procurement that are currently uncovered by Buy America. And it is important for two reasons. One is the reason that you suggest, which is that it affords the opportunity of State-owned enterprises and others to gain access to our market with the leverage of American tax dollars.

Second, and I think this is fundamentally the most important thing, our procurement market is one of the most open in the world and it is also out-sized. In fact, it is disparately out-sized compared to the next five OECD partners in terms of public procurement markets. And so we have opened ourselves up to these imports coming in, in many cases subsidized or coming from State-owned

companies without any sorts of protections. And we more or less stand alone in that regard.

We need to modernize our laws and we look forward to working with you to do that.

Senator BROWN. Thank you, and one more question for Mr. Paul. My concern, as I said in my opening statement, with CRRC and BYD is not with the American workers they employ but with the Chinese Government's influence and control and the resulting effects. In fact, I am worried that American workers' jobs may be at risk if and when these companies consolidate market share—really coming from the admonition and the warnings from Ms. de La Bruyere, I think she said that just perfectly—but worried that those companies consolidate market share and relocate their production back to China.

What would a Chinese State-owned or State-controlled company captured industry, what is likely to happen?

Mr. PAUL. Overall in the industry, and particularly as they gain market share—and I want to point out quickly here that I think CRRC now has about 83 percent of global rolling stock company. When you are squeezing out competitors, that consolidates supply chains. And what that means is that in that supply chain, up and down it, you are going to lose jobs.

We have seen this already. There was a story just within the last month that kind of boiled my blood. And that is the fact that the metal shells for these CRRC cars that are coming into Massachusetts are being built in China with subsidized steel at a time where our industry is still under a great deal of stress and where we have seen layoffs recently and we will see them, for instance, at U.S. Steel in Michigan.

So the fact that tax dollars are being utilized for this purpose is something that should be outrageous to elected officials.

I was a shop steward for a union I served in, and so I believe in the dignity of work. And I do believe that instead of trying to play the victim here, I think what we need to find is that if these are productive assets that BYD has and CRRC has, there should be willing private sector buyers that would be able to take those on to provide true competition for the American market.

Senator BROWN [presiding]. Thank you. Chairman Crapo and I were talking briefly before the hearing. We have very difficult political philosophies. We work together on a lot of banking issues like anti-money laundering and issues like that. We do not see the world the same way on big issues.

We both had voted against the NTR 20 or so years ago. And just, people were sounding the warnings that we were outsourcing so much of our production. In some sense, we helped to create, upon intensive lobbying by some businesses, a whole new business plan where you shut down production in the U.S., you move to China, and then you sell back into the U.S. And we have, in a sense, given that away.

And it is—mixing metaphors—these roosters are coming home, or whatever. Chickens, I guess, come home to roost. Roosters probably come with the chickens when they come home to roost, but anyway.

Senator McSally.

Senator MCSALLY. Thank you, Ranking Member Brown and Chairman Crapo, for having this very important hearing. I appreciate the testimony of everybody here today.

When I was a cadet at the Air Force Academy in 1984, we were studying Sun Tzu and China's plans to dominate the world. And we are seeing it manifest before our eyes in every possible facet of power for them to become a world dominant power and supplant us. So thank you for your important testimony today.

I am pretty sure I know the answer to the first question but does anybody on this panel think China is our friend here? Anyone?

[No response.]

Senator MCSALLY. No, right? I could not agree more.

Look, I have been focused on national security my whole life. I very much appreciate the importance that you are putting on this from a national security point of view. Look, they are going to use all means necessary and it is right in front of us. We are seeing what they are doing in the military. We are seeing what they are doing with supply chains which has been highlighted with coronavirus and our pharmaceutical industry. We see it with our important critical minerals. We are addressing that on Energy and Natural Resources. We see it in the tech industry. We see it in big data.

And now today we are talking about public transportation and how this is a part of their global plan. And you do not have to just believe me or believe you, you just can read what they say, which you have all cited it, whether it is Made in China 2025 or their transportation great power strategy, which is a subset of that. It has all been cited today.

I think all of your testimony needs to be required listening by every State and local bureaucrat who is involved in public transportation, who may just think they are doing their job to bid out to the lowest bidder for local transportation and save money. But as you said, Frank, and it is great to see you again, the cost of not addressing this and stopping this from happening is astronomical to our national security, the cost to our taxpayers. This is just so troubling to me and I so appreciate your raising awareness on it.

We have a platform here, too, so I am making a plea. To my fellow Americans, the State and local bureaucrats, wake up! We are being played by the Chinese Community party. I am not a fear monger. This is exactly what is happening, and this is the unclassified version of what is happening here.

So thank you for all you are doing here.

With what has been brought out today, I guess my question is with this 2-year delay, which we all think is a bad idea, is there any barrier for States and localities from simply just doing the right thing? Forget about waiting for Federal guidance on exactly what they can and cannot do, is there any barrier right now where there are bids going on right now for the next project, for a local government to say no, we are not going to allow the Chinese-owned company to win this bid? We are going to do the right thing and we are going to comply by this law, but we are also going to do what is best for America, what is best for American workers and what is best for our future and our security? Is there any barrier to that?

Mr. O'MALLEY. Senator, I think you have touched on it exactly, and let me give you an example. In Atlanta, over the last couple of years, they had a major bid for several hundred railcars. And that is actually a new company that has come in, European owned and made a major investment in the State of Utah. They are going to be employing 1,000 people by the time they are done with that.

Senator MCSALLY. Right, exactly.

Mr. O'MALLEY. That is exactly what should be happening.

And so no, I do not think there is any real barrier. And to the extent they had an issue before December, certainly I do not think they should at this point. Use your discretion and do what is right.

Senator MCSALLY. They do not need to wait for guidance; right? I would ask the rest of you to weigh in.

Mr. PAUL. Senator, that is a good question. And unfortunately, the companies we are talking about here, CRRC and BYD, have been proactive both anecdotally and through news reports of reaching out to these agencies, in some cases mischaracterize what the obligations—

Senator MCSALLY. It is called propaganda. That is what the Communists do.

Mr. PAUL. Right. And unfortunately, under some of the contracts that are set up they have options for ongoing purchases that—again, I think that is an area that needs to be tightened up because if a local agency has a lowest best bid requirement and they are operating under no other information, CRRC and BYD may persuade them to continue a contractor to have a contract that has options that go beyond the 2-year term.

So I think it is incumbent on the Congress, as well as the agencies, to weigh in on that and to ensure that the intent of the law is what is being implemented right now.

Senator MCSALLY. Thank you. Ms. de La Bruyere.

Ms. DE LA BRUYERE. I just wanted to add, it is not just doing the right thing. It is also in their best interest.

Senator MCSALLY. Right.

Ms. DE LA BRUYERE. In the immediate term, BYD buses break down. In the longer term, they break down the industry in that area.

Senator MCSALLY. Great, thanks.

Mr. CILLUFFO. Senator McSally, great to see you again.

A very, very quick point. I mean, thus far I think we have all said, in one way or another, China's strategy has honestly been powered by theft of U.S. intellectual property.

Senator MCSALLY. Right.

Mr. CILLUFFO. I am worried about the day they stop stealing our secrets. The reason I say that is because they have already—

Senator MCSALLY. They do not need to. They have coopted.

Mr. CILLUFFO. —gotten everything they need and they are putting that toward marketing. And I think there is a little bit of hubris, we still think they are imitators. They are not. They are innovators now and they are investing so heavily in certain technologies such as quantum computing, artificial intelligence, through an authoritarian regime lens. So I think we need to heed that and take that seriously.



Senator MCSALLY. Great. Thank you. And I know I am out of time, but I do want to highlight, in Tucson they did recently receive an FTA grant, went to a company, an American company, American-owned, American-made. This is the right model and I want to highlight the good job they did there.

Thank you, sir.

Chairman CRAPO [presiding]. Thank you.

Senator WARNER.

Senator WARNER. Thank you, Mr. Chairman.

I want to thank you and the Ranking Member for holding this hearing, on this very important issue. I think this is one where there is broad bipartisan agreement.

As somebody who sits on the intel side, and we have now done more than a dozen classified briefs to various sectors of the industry, recognizing this emerging challenge. Frankly, it is a challenge on an economic basis that I would argue is much greater than the Soviet Union ever was.

The only caveat I would put on the front end, I think we have to be careful when we talk about this to say that we are anti-Xi Jinping, anti-Communist Party of China, that we are not anti-China because particularly in this country there are a whole lot of Chinese Americans who hear these comments and believe that this is venom, anger, frustration directed at them. We have to be very, very careful about that.

The point I always try to make is I actually stand with the Chinese people. I stand with the people of Hong Kong against the kind of authoritarian practices that this regime practices both in terms of surveillance and also some of its business practices.

You mentioned what is happening in 5G. As somebody who has taken the lead on this, Huawei is a national threat. And the truth is there is not going to be a market-based solution when Huawei gets 40 percent of the 5G market by controlling the Chinese market and \$100 billion backstop. There is no market base where other Western competitors can be competitive against that.

The Chairman mentioned the fact about IoT. One of the areas that we are finally making some progress on but it is insane that it has taken 3 years is the Federal Government, dismissing all of the State and local activities, buying literally billions of IoT connected devices a year and we still do not have even de minimis security standards on those devices such as making sure they are patchable, making sure there is no embedded passcodes.

We finally have Federal legislation that will at least mandate on Federal spending that you have minimum security devices. It is lunacy that it has taken us 3 years and that there has been internal disputes between various standard setting bodies about who is going to set the standard. We need the standards yesterday.

Again, all bipartisan. This is one of the issues where I think there is absolutely no difference.

On this particular topic, I just want to simply echo the good work Senator Baldwin did, the Chair and the Ranking Member. As somebody who, along with Senator Van Hollen and Cardin and Kaine, started to take the lead when we saw the challenges that WMATA may be going down, frankly where other transit systems have already gone down. And as the testimony has pointed out,

this is not only potentially the ability to create havoc with these cars but the ability to monitor American's conversations, where they are. Again, these cars are complete with literally thousands if not millions of sensors that are IoT connected. And I think it is very appropriate that we have backed WMATA off, that we have taken and put these kind of restrictions in place for hopefully, on a going forward basis, all transit systems. But we do need to do more.

Mr. Cilluffo, I want to ask you, one of the things I have also been working on is cybergrants to State and local officials because we do need to make sure that we bring this expertise all the way up and down, not only the private sector supply chain but within the State and local government ability as well. Could you speak to that for a moment?

Mr. CILLUFFO. Sure. Thank you, Senator Warner.

I recently had the opportunity to testify before your House colleagues on State, local, tribal, territorial, and cybersecurity needs. You are absolutely right. The challenge we see at the Federal level pales in comparison as to what we see at State, local, tribal, and territorial.

So I do think there is—we need to better enable and support—sort of think of it as a Geek Squad, whether it is through the Cyber and Infrastructure Security Agency at DHS to be able to enable some of those capabilities. They are starting at a very low baseline. And when you look at the talent needs with respect to cyber, obviously the Government in any form cannot compete with the private sector.

But when you start looking, State and local is unfortunately further down the totem pole. So we have to come up with new ways, whether it is enhancing scholarship for service programs to be able to allow them to work at State and local. That is a dire need and one that needs to be backfilled yesterday.

Senator WARNER. I would just simply say to the Chairman as we wind down, that I appreciate what you are doing here. Clearly, in terms of public transit we need to make these restrictions. But we need to work together, as well, on IoT, on 5G. And frankly, as we think about potentially governmental action to support American or Western-based, we have got to figure out how to get it right in 5G because we may have to do the same thing in artificial intelligence, quantum computing, facial recognition, and a host of other areas.

Thank you.

Mr. CILLUFFO. Senator Warner, can I just raise one quick—because this is what makes cyber so vexing. It transcends all committees. It transcends all sectors. And it touches everyone's responsibility, that we do need to think about this issue a little differently than we do many of the other issues.

So if I am transportation, I am dependent upon telecommunications. I am dependent upon the electric, the grid, and energy sectors, oil, gas, water. So it is looking at those interdependencies that I think is so challenging but so important.

Senator WARNER. Amen.

Chairman CRAPO. Thank you, very good points.

Senator TILLIS. Thank you, Mr. Chairman, for holding this Committee. And thank you all for being here.

I am sorry, I had to step out before your opening statements were complete. I was down at a Senate Armed Services hearing, hearing from the Department of the Navy, getting ready for our NDAA markup. And guess what came up? China, a country—to the point that was made—at one point we only worried about China because they could beat us in quantity. They could put out more platforms. But we could beat them on quality.

But now, they are innovators and they are closing the qualitative gap, and they already have an advantage on the quantitative side. And this sort of stuff is funding that.

While we go and make a penny-wise pound-foolish decision about passenger cars or electric buses, we are literally giving to the Communist regime the very resources they need to threaten us, expand our standoff distances, and threaten American men and women across the globe.

If you take a look at some of the major transit authorities up in the Massachusetts area, Pennsylvania, Chicago, Los Angeles, they are buying these passenger rail vehicles. They have been proven to not be at the level of quality that we would expect. I do not even know what the total cost of ownership is but my guess is if you looked at the total cost of ownership and you were making smart strategic sourcing decisions, you probably would not buy them, particularly—if all things were equal—when you know that these are resources that are going right back to the Chinese Communist party.

There is no such thing as a private company in China. There is no such thing.

We have to have people wake up. I see an *L.A. Times* report that I think agency staff described the buses as being unsuitable, poorly made, and unreliable for more than 100 miles.

The threat to our industrial base is not hypothetical. How many of you are familiar with what China did over several years in Australia? Starting with low-cost passenger rail with the promise to manufacture it in Australia. Now they are sending shrink-wrapped commuter railcars to Australia. Destroyed that part of the base. And then making the play on freight rail, which is absolutely a threat to our national interest.

So does anybody there, in a couple of minutes, want to talk about how China has systematically disintermediated the industrial base in Australia? And if we let them continue to do it, they are going to do it here. It is going to cost American jobs, but I do not think it is hyperbole to say that at some point it could cost American lives. And those are the lives of men and women in uniform.

We will just go down the line if you all want to touch on it in my remaining time.

Mr. O'MALLEY. So Senator, I think you are absolutely right. In Australia, they completely wiped out the domestic manufacturing capacity.

Senator TILLIS. They did not start that way.

Mr. O'MALLEY. Absolutely.

Senator TILLIS. They promise they were going to keep them in there and keep those Australia jobs, and now they are gone.

Mr. O'MALLEY. Sounds very familiar. And so I think we absolutely do not want to see that happen here. Right now the rail supply sector is heavily domestic and our companies here are manufacturing, they are not assembling these products here. That is a critical difference in terms of what we are seeing the CRRC.

In addition to all of the national security issues involved, but when you talk about assembling, there are far fewer jobs. We question whether they are fully compliant with Buy America as they do that. And quite frankly, it is just not in our long-term interest. I think you are absolutely spot on.

Senator TILLIS. Mr. Paul.

Mr. PAUL. Senator, I agree with everything that Mr. O'Malley said.

I would also just add this, that the public procurement market alone are not going to float BYD or CRRC. But the important thing is they are using these tax dollars to gain a beachhead into important industries in the United States. And as large as our public transportation sector is, the private transportation sector is exponentially larger.

And BYD has the ambitions to be the globe's leading electric vehicle maker. And they have targeted the American market.

And so the fact that they are using tax dollars to go at essentially what is one of the keys of American manufacturing—one out of every nine manufacturing jobs in the United States is tied to the automotive sector.

There are many things that Congress should or should not do. It should definitely not allow a company to use tax dollars to gain leverage into one of the keys of American manufacturing like that.

Ms. DE LA BRUYERE. It is not just that they have done that in Australia. They have also done that in the U.S. This is the story of the semiconductor supply chain, of the tire supply chain, of the steel supply chain. But it is also the story that moves up a step in all of those supply chains. And as China cements its position there, then moves up a step in the next kind of supply chain.

Because this is the question of innovation, too. Sure Beijing “innovates”, in quotes. But they innovate by siphoning our innovative resources so that it is not only our taxpayer dollars that are fueling them but it is our innovative resources that are allowing them to coopt 5G and the Internet of things and space and whatever we are describing when we talk about AI. And that is a way bigger subversive problem.

Mr. CILLUFFO. Senator Tillis, excellent question and I will be very brief. We always want to learn from our mistakes. Even better to learn from the mistakes of others. And I think the lesson is loud and clear in Australia.

But let me just underscore one point. They have learned themselves. They are standing tall and firm on the 5G Huawei question in terms of the next set of critical infrastructures. And I think it is the hard lessons they have learned in the rail sector.

So they are standing shoulder to shoulder with us on that particular issue, but you are spot on.

Chairman CRAPO. Thank you.

Senator Smith.

Senator SMITH. Thank you very much, Chair Crapo, and also Ranking Member Brown. And thank you all so much for being here. As you can tell, many of us on this Committee are very interested and very concerned about how Chinese-funded State-backed enterprises are aiming to dominate global manufacturing of new energy vehicles.

And for me, I am particularly interested in buses because in Minnesota we are the home of two New Flyer manufacturing plants. I will share this with my colleague, Senator Jones. One is in St. Cloud and one is in Crookston.

New Flyer supports approximately 1,200 jobs in Minnesota, many of them good union jobs with CWA, and very important to the economy of these two communities.

I joined some of my colleagues last year in working on this defense authorization bill, which included a provision that I authored, which would prohibit Federal transit funding from being used to purchase buses and railcars that are manufactured by Chinese State-owned and State-supported enterprises.

I am looking at Mr. Paul, but I am actually going to direct my first question to Mr. Cilluffo. Can you just explain, help us understand why this provision that we worked on is not only about American jobs but it is also about—how does it relate directly to national security, when we are thinking about these buses?

Mr. CILLUFFO. Thank you, Senator Smith.

And I think the procurement acquisition piece is critical but, in itself, is insufficient.

So from a mission assurance perspective, which DOD would zero in on, the ability to enhance and maintain our military capacities you do have the potential to disrupt our ability to move people, goods, and things.

Senator SMITH. Right.

Mr. CILLUFFO. In a time of crisis, that could be devastating.

So basically, there are three things: computer network attack, disruptive and/or destructive attacks; computer network exploit, espionage, intellectual property theft, or political or any other form of information theft; and then just the fact that the products themselves could be pretty shoddy. So you have got a combination of all three that I think factor into that national security argument.

Senator SMITH. Thank you, that is very helpful.

Mr. Paul, you talked in your testimony about this compliance with Buy American laws, and Senator Brown referred to this, as well. And I completely agree with you that taxpayer funds should be going to U.S. companies to create American jobs instead of going overseas to foreign companies.

It is interesting how this applies in the area of buses and batteries. Back in 2018, Senator Jones and I, with Senator Stabenow, asked the Federal Transit Administration to look into this. We asked the FTA to review whether Buy America requirements need to be updated, to make sure as we think about this relates to battery electric power buses. So we are still waiting. That review is not finished yet.

But I would like if you could just help us understand this. Can you clarify how Buy America requirements are applied to battery electric transit buses? And whether you think that the current reg-

ulations are sufficient to protect domestic manufacturing in this area?

Mr. PAUL. Senator, it is a great question. And first of all, the way in which it is being applied now is not sufficient to protect American jobs. Those standards have not been updated since, I believe, 1996. Obviously, a lot has happened in the electrical vehicle industry since that time. And so there is a desperate need to do it.

It should be done in a manner that does not favor one proprietary system or another but there are, in fact, as you indicated, some American based bus suppliers that could compete. The challenge with Buy America compliance—I mean, there are questions, first of all, whether BYD actually is complying. An Inspector General's report from Albuquerque, New Mexico, points to that, and I would recommend that to your attention.

But the second thing is the manner in which the batteries are classified right now account for an extraordinary amount of the value of the vehicle. That means that a lot of the other parts of the vehicle that BYD is assembling in California are coming from China. Everything from the doors to the tires to everything else. And so it is eroding the impact that Buy America laws are supposed to have.

Eventually, we want to get to a point where batteries are American made and vehicles are American made and that standard is moving up. But that is not where we are right now.

Senator SMITH. I completely agree with you, particularly when we think about how important I think it is for America to be leading and not following when it comes to battery technology. And so here we have a situation where you have got a component of a component of a component in the battery that is driving these buses. And it is fundamentally Chinese made, yet they are able to claim it because of these outmoded rules, as I understand it, as an American component. And that seems to be going directly counter to what it is that we want to be accomplishing. And it hurts American manufacturers like the one in my State.

Thank you very much.

Chairman CRAPO. Thank you.

Senator JONES.

Senator JONES. Thank you, Mr. Chairman.

Thank you all for being here today.

Mr. Cilluffo, is that how you pronounce that?

Mr. CILLUFFO. Right.

Senator JONES. War Eagle.

I want to stick with transit a little bit. In 2017, the U.S. Army and Navy discovered an electronic back door to the Chinese in drones made by a Chinese manufacturer, DJI. So they ordered soldiers and sailors to discontinue the use of those drones due to the concerns of cyberspies were intercepting video and other encrypted data of our U.S. military personnel.

There is a clear connection to Chinese actors in both the drone example and the scenario in your testimony detailing how they could exploit and weaponize transit systems. I am clearly afraid that bad actors might use information gathered from buses and railcars to coordinate specific cybersecurity attacks.

As the technology gets more innovative and is incorporated into these smart buses and railcars, are you concerned that these vehicles and their passengers as they are communicating, whatever it is, that we are going to be sending Chinese data from all of these? Particularly, I mean you have got the Tiger Transit System down at Auburn with all these kids and the faculty riding around and they are on these dang things the whole time. Same thing at the University of Alabama and all around the country.

Should we be concerned about that?

Mr. CILLUFFO. About the University of Alabama? I am kidding.

Senator JONES. I know Auburn is always concerned about the University of Alabama.

[Laughter.]

Mr. CILLUFFO. Senator Jones, thank you for all you do for Auburn and War Eagle and the State of Alabama.

Yes, you know, I did have the opportunity to testify on DJI and UAS and drone activities. And there was a very real concern that ET is phoning home. If you have a remote access to be able to gain in, you can control that data. That does not mean it is always happening. I do not have the smoking keyboards and smoking guns for everything but the capability exists to do just that.

So yes, I do think, in addition to what I would consider the higher end national security issues we need to get our arms around in terms of mission assurance and some of the disruptive and destructive attacks, yes. Theft of data and information of any kind.

I am sure many in this room were victims of the OPM hack. This was at the U.S. Government. Imagine if you start matching up OPM data with other data that has been gleaned through other means in addition to biometrics. That is a scary place.

And we tend to mirror image. We tend to look at it through a democratic lens. Authoritarian regimes handle and treat this information very differently.

Senator JONES. Thank you.

This is really for the entire panel or anyone on the panel. When States and local communities buy buses and materials for transits they tend to opt for it through a bidding process. They just go to the cheapest option. So State-owned enterprises, including all the ones in China, benefit from those subsidies. It puts American manufacturers at a disadvantage.

However, States and communities making procurement decisions are just not always armed with knowledge that certain companies are State-owned enterprises. They might change their modeling a little bit if they were aware of that.

So my question is what tools exist to help local communities identify and determine if companies have connections to a foreign Government, especially countries like China or any other autocratic ones? Yes, sir. Mr. Paul.

Mr. PAUL. Senator Jones, thank you for the question.

They have very few tools at their disposal, particularly smaller agencies that are already cash-strapped. You have seen obviously a bigger—you know, the rail transit system is much more compact in the United States and much more urbanized than buses which are, again, on college campuses, at every airport you go to, and

throughout midsized cities. And fundamentally, these agencies are not armed with the information that they need.

That is why it is important that the Department of Transportation provide guidance and do active outreach as soon as possible to ensure that this law is fully implemented. And to date, we have seen absolutely no steps taken toward that.

I want to thank the Senator and the Committee for having the hearing because we need to drive this process along. We cannot expect a mid-sized city to be able to know everything that Beijing is doing. That is one of the obligations we have here.

Senator JONES. Let me follow up on that real quick in my remaining seconds, if you will give me a little bit of leeway, Mr. Chairman. I do not like to create Big Brother around here anymore than anybody else does, but would it help to create some kind of database, a secure database, where Federal departments and agencies can share identifying information of adversarial State-owned enterprises, related entities with close ties to foreign Government or anything? Is that something that we ought to explore in Congress, creating that database?

Mr. PAUL. I would say that sounds very reasonable to me, along with extraordinary guidance provided along with federally funded grant opportunities for these local agencies. It is important that we do this sooner rather than later because what we have observed in both the bus and the rail sectors is that BYD and CRRC are actively trying to get business now under this 2-year window and to seek it with options so that it erodes the effectiveness of the restrictions that Congress is attempting to put into place.

Senator JONES. Great. Do you want to say something?

Ms. DE LA BRUYERE. Yes.

Senator JONES. Assuming that the Chairman will let you.

Chairman CRAPO. Briefly.

Ms. DE LA BRUYERE. I will be quick.

It is also not just China's State-owned companies, and so the need is also that the Federal Government be able to monitor better what the various subversive links that are not currently triggered by our monitoring processes are. So that is like State-supported companies like BYD but it is also investment in what appear to be U.S. companies, shell companies, and other sorts of opaque links.

Senator JONES. Great. Thank you. Thank you for the extra 1 minute, 24 seconds.

Chairman CRAPO. You are welcome. That does conclude our questioning and I want to also again thank the witnesses, not only for your testimony today but you have been engaged on this for a long time and your work has been very helpful to the Committee. I think we have delivered a very strong message today. I appreciate you helping us to do so. For Senators who wish to submit questions for the record, those questions are due on Thursday, March 12. I encourage the witnesses to respond to those questions as promptly as you can. Again, thank you all for being here, and the hearing is adjourned.

[Whereupon, at 11:31 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]



### PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

Today's hearing will focus on the threats posed by State-owned and State-supported enterprises on public transportation.

Last year, Ranking Member Brown and I were original cosponsors with Senators Cornyn and Baldwin in introducing S. 846, the Transit Infrastructure Vehicle Security Act, language that served as the basis for Section 7613 of the National Defense Authorization Act, or NDAA, which was enacted in December.

As you will see today, this issue has broad bipartisan support.

There are 52 bipartisan cosponsors of S. 846, and more than half of the Members of this Committee, on both sides of the dais, are among that list.

The provisions in S. 846 are also supported by the Trump administration, both in a Statement of Administration Policy regarding the House NDAA, and Acting OMB Director Russell Vought's letter to House and Senate Armed Services Committees supporting the language ultimately reflected in Section 7613.

Today's expert witness panel reflects the multifaceted nature of threats BYD and CRRC pose to our national security, the economic competitiveness of the domestic bus and rail manufacturing industry, and cybersecurity.

All of the witnesses have been valuable resources to the Committee as we got the language of S. 846 enacted into law, and we thank them for their expertise and willingness to help.

From a national security perspective, 15 former generals and admirals from the Energy Security Leadership Council wrote a letter warning of the Chinese strategy to dominate critical industries.

The former military leaders stated that the "Chinese industry is inexorably intertwined with Chinese Government, which creates a host of economic and national security concerns for the U.S."

Economically, both CRRC and BYD include direct subsidies from the Chinese Government in their annual reports.

There are presently at least seven other transit railcar manufacturers besides CRRC and at least five other transit bus manufacturers besides BYD in the United States.

It is impossible for other bus and rail manufacturers to fairly compete when these two companies have the unfair advantage of the financial support of the Chinese Government.

As transit agencies are working to address the 98.8 billion dollar state of good repair backlog in the industry, they are often looking to modernize, such as transitioning to electric buses and incorporating autonomous technologies.

Along with the modernization comes increased connectivity, which increases the threat of cyberincidents and espionage.

The language enacted in Section 7613 of the NDAA acknowledges that all of these threats are real, and applies significant new restrictions on funding for the acquisition of CRRC railcars and BYD buses.

It is unfortunate that Section 7613 includes a 2-year delay on the prohibition, and it is critical that transit agencies immediately understand the threats associated with purchasing from a State-owned or State-supported entity, and how that should affect their procurement decisions now and looking ahead.

Recently, Senator Brown and I, along with House Transportation and Infrastructure Chairman DeFazio and Ranking Member Graves, wrote to Secretary Chao emphasizing the urgent need for the Department of Transportation to put out information online or issue a "Dear Colleague" so that transit agencies are informed of the new law and can plan their rolling stock procurements accordingly.

We have already heard anecdotally that both BYD and CRRC have been seeking to misinform agencies as to the applicability of the language.

In order for agencies to make informed procurement decisions, it is critical that the Administration respond and give transit agencies the tools they need to understand how to comply with the statute.

---

### PREPARED STATEMENT OF SENATOR SHERROD BROWN

Thank you, Mr. Chairman, for calling today's hearing on a bipartisan bill that you and I, along with Senators Cornyn and Baldwin and 48 others, successfully included in the National Defense Authorization Act at the end of last year.

I want to welcome Senator Cornyn and Senator Baldwin, our partners in the Transit Infrastructure Vehicle Security Act. I also want to thank the many Members of this Committee who supported and cosponsored the bill.

Our Committee's bipartisan work to address a threat to public transportation from companies supported and controlled by the Chinese Government shows that

our Government can be nimble in responding to new economic and security threats. We must be vigilant. It's why just this week, Senators Cornyn, Baldwin, Crapo, and I have sponsored an amendment to the energy bill on these issues.

While TIVSA is now law, we need to keep our focus on the two Chinese companies in question: CRRC and BYD. These companies have repeatedly shown that they do not play by rules.

Let's talk first about CRRC. As a State-owned enterprise, CRRC didn't have to worry about making a profit when it used lowball bids to win four major U.S. contracts for transit railcars.

In 2014, CRRC offered a bid on the Boston MBTA contract that was more than \$150 million lower than the next competitor. In Chicago in 2016, they beat the next lowest bidder by \$226 million.

That's not because they were doing the work more efficiently—it's because they were being propped up by the Chinese Government. So it's not surprising that established manufacturers were unable to match these bids.

But that isn't even the full picture of the damage from CRRC's lowball bids.

Hyundai-Rotem manufactured railcars for Philadelphia's SEPTA system and Denver's RTD system. The 300 Hyundai workers in its Philadelphia factory were represented by Transport Workers Union Local 234, and they made a middle-class living wage with employer-provided benefits and a retirement plan. All of these workers lost their jobs after Hyundai-Rotem lost the SEPTA contract to CRRC.

Hyundai closed the plant in August of 2018. For every U.S. job created by CRRC, it's estimated the U.S. loses between 3 and 5 jobs.

Before Congress acted last year, CRRC was making plans to win a contract with the Washington, D.C., Metro worth more than \$1 billion dollars.

And then there's the electric bus maker BYD, another company covered by TIVSA. I want to be clear—my concern with CRRC and BYD is not with the American workers they employ, but with Chinese Government's influence and control.

BYD may not be technically owned by the Chinese Government, but it's certainly controlled by it. As our expert witnesses will testify, BYD may receive even more State support than CRRC, and BYD has deep ties to the Chinese Government.

BYD's goals in the U.S. extend far beyond the public transportation market. BYD supplies electric trucks for freight delivery, it offers electric garbage trucks to cities, and it's eyeing the passenger car market.

There are four other major bus manufacturers that build electric buses in the U.S., and two are American-owned. These companies are ramping up their production of zero-emission buses to help American transit agencies reduce emissions, but they do not enjoy enormous support from the Chinese communist party.

This is an industry of the future—we can't cede it to China.

BYD likes to point out that Warren Buffet is an investor in their company. One billionaire investor does not mean that BYD is looking out for the interests of American workers.

CRRC and BYD are two in a long line of examples of how China cheats its way into being a global leader in industry after industry. Ohio's steel industry knows that all too well.

For years, Chinese State-owned steel companies have been flooding our market and the global market, and forcing U.S. steelworkers out of their jobs.

It's why we've taken more than 60 trade enforcement actions against Chinese steel producers, to help create a level playing field for American producers.

But CRRC and BYD undermine those trade enforcement efforts by purchasing Chinese steel, turning it into frames and shells for buses and railcars at factories in China, and then shipping them to the United States for final assembly—and they get bought using taxpayer dollars, threatening our steelworkers.

It's exactly the kind of cheating you'd expect from those Chinese companies that refuse to play by the rules.

It's a jobs issue, and it's also a national security issue.

When we let Chinese companies manufacture our buses and railcars, we also face cyber and data security risks. Our hearing today will discuss these concerns facing transit agencies and our broader transportation sector. TIVSA created an important new requirement for transit agencies to assess cybersecurity risks, but Congress still needs to fully assess the risks associated with data from our transportation system being exposed to foreign actors.

We also know the threat of Chinese State-owned enterprises investing in the U.S. isn't limited to rail and bus manufacturers. We don't even know all the ways in which companies owned or controlled by the Chinese Government are gaining footholds in our market.

My legislation with Senator Grassley—the Foreign Investment Review Act—would require the Secretary of Commerce to review certain foreign investments, par-

ticularly those made by State-owned-enterprises, to make sure they are in the long-term, strategic interests of American workers and American businesses. This is just another example of bipartisan legislation that can help address new economic and security threats.

I will close by noting that as we work to reauthorize transit programs, we need to strengthen Buy America requirements. It's not complicated: American tax dollars should be support American jobs.

Thank you, Mr. Chairman.

---

#### PREPARED STATEMENT OF SENATOR TAMMY BALDWIN OF WISCONSIN

Chairman Crapo and Ranking Member Brown, thank you for the opportunity to be here today to discuss our legislation, the Transit Infrastructure Vehicle Security Act, which became law in December 2019 as part of the National Defense Authorization Act for Fiscal Year 2020.

This law is important to me in short because Wisconsin is a State that makes things. For generations, we have assembled our Nation's ships, built our Nation's engines, and brewed our Nation's beer. However, since we allowed China to enter the World Trade Organization in 2001—a move I opposed—millions of manufacturing jobs have been lost. And many workers have seen their wages stagnate as a result of downward pressure from competition from Chinese State-backed companies.

As a nonmarket economy, China gives hundreds of billions in State subsidies to manufacturers in industries in which the Government wants to compete. In 2015, the Chinese Communist Party released a strategic document outlining how it intends to compete globally in manufacturing called "Made in China 2025".

This plan revealed that China desires to dominate in railcar and electric bus manufacturing. Recently, two State-supported companies have made in-roads into the U.S. market, the railcar manufacturer China Railway Rolling Stock Corporation (CRRC) and the bus and electric battery manufacturer Build Your Dreams (BYD).

We know from observing CRRC's entry into the Australian market that domestic industry cannot compete with China's aggressive State-owned enterprises. Over the last 15 years, Australia's domestic railcar production collapsed as CRRC gained increasing market share.

Wisconsin manufacturers are happy to compete with anyone in the world, but they need a level playing field. China's nonmarket economy forces Wisconsin manufacturers to compete with Chinese companies that get free land, free utilities, free R&D, and interest-free loans worth hundreds of millions of dollars.

These Chinese Government-subsidized rivals would be bad enough, but now these companies are increasingly using their U.S. assembly facilities to win taxpayer-funded contracts from the Federal Transit Administration to procure buses and railcars for American cities.

When taxpayer dollars are spent, we must make every effort to ensure they support American workers and businesses. As a strong supporter of expanding and improving Buy America requirements, I was proud to join Senators Crapo, Brown, and Cornyn in introducing and passing legislation to prohibit FTA funds from going to companies supported by nonmarket economies, such as BYD and CRRC.

In 2 years, the prohibition in the law will go into force. Transit agencies need to know how they will be affected as soon as possible. Senator Cornyn and I have both requested that Secretary Chao and Acting FTA Administrator Williams publish information to ensure that transit agencies planning for the future are able to make safe, informed, and legal procurement decisions.

While the legislation addressed many immediate concerns facing domestic railcar and bus manufacturing, I urge the Committee to work with the Department of Transportation to further tighten Buy America requirements to ensure that Federal taxpayer dollars support good-paying manufacturing jobs in the U.S. I am deeply concerned by a study from *Oxford Economics* that found that CRRC's railcar production in the U.S.—while compliant with Buy America—relies heavily on imported parts. The report estimated that—as a result of this "import and assemble" business model—every one job CRRC creates in the U.S. eliminates as many as five U.S. jobs.

I will close by commending the Committee on the oversight work it is doing to ensure that this law is implemented as swiftly and as effectively as possible and once again thank the Chair and Ranking Member for the opportunity to testify here today.

### PREPARED STATEMENT OF SENATOR JOHN CORNYN OF TEXAS

Thank you Mr. Chairman and Ranking Member Brown—I appreciate you inviting Senator Baldwin and I to share our thoughts with the Committee. This issue is important to my home State, our national security, and the integrity of our economy.

China has a long history of undermining market economies across the globe by subsidizing Chinese businesses so they can outcompete domestic industry, because they never have to worry about turning a profit.

Global domination of rolling stock production, like trains and buses, is at the forefront of the “Made in China 2025” initiative, which outlines the Chinese Communist Party’s plans for economic domination across the globe.

This is why I was concerned when I found out certain Chinese State-controlled companies like the China Railway Rolling Stock Corporation (CRRC) and Build Your Dreams (BYD) were submitting unrealistically low bids for transit projects in major U.S. cities in an attempt to put competition out of business and dominate the market on a long-term basis.

Transit railcars and buses are highly advanced vehicles equipped with a host of computers, sensors, and cameras.

When Americans step onto a subway or city bus, they accept that many of these devices are there to ensure their safety and trust the Government won’t abuse their civil rights.

But these advanced technologies can do much more than help you get to work on time. They’re also capable of spying on passengers and our infrastructure network—and they can be undetectably placed on transportation systems across America.

Thousands of Government and military officials use transit services every day, especially here in D.C. I’m sure many of the folks in this room relied on those trains and buses to get here today.

The potential for an adversarial State actor to monitor the movements of American citizens, hack personal or Government-issued devices, and collect intelligence on our military is a major security concern.

Allowing American trains and buses to become Trojan horses for these technologies on American soil is unacceptable.

And I think we can all agree that Chinese State-controlled companies should not receive a dime of American taxpayer money in their efforts to control our economy and undermine national security.

Fortunately, Congress has taken critical action to address the problem.

Senator Baldwin, Chairman Crapo, and Ranking Member Brown joined us in getting the Transit Infrastructure Vehicle Security Act passed into law as part of the National Defense Authorization Act last year.

This commonsense, bipartisan law sends a strong signal to the Chinese Government that we will not allow them to infiltrate the operations of our critical infrastructure.

The legislation will ban the use of Federal transit funding for the procurement of railcars and buses produced by companies that are owned, controlled, or sponsored by foreign Governments with nonmarket economies and that are designated as countries of concern by the U.S. Trade Representative.

Unfortunately, special interests were able to demand a 2-year enforcement delay of some of this legislation’s critical components.

I am here today to ask for your help in ensuring this delay does not turn into a window the Chinese Communist Party and its State-controlled companies can further exploit by rushing to procure contracts and extending their tentacles further into America’s infrastructure network.

Without strong leadership from the Federal Transit Administration, transit agencies will unknowingly allow CRRC and BYD to compete for their projects, even though a Federal ban on such contracts is coming soon. We must do everything we can to stop this.

I look forward to working with Chairman Crapo, Ranking Member Brown, and other Members of this Committee to educate Government agencies, the public, and our local jurisdictions about China’s threat to our infrastructure—and the legal tools Congress has enacted to address this problem.

### PREPARED STATEMENT OF E. MICHAEL O’MALLEY

PRESIDENT, RAILWAY SUPPLY INSTITUTE

MARCH 5, 2020

Chairman Crapo, Ranking Member Brown, and Members of the Committee, thank you for the opportunity to testify today on the threats facing public transportation

systems from foreign State-owned and State-supported enterprises, an issue that is of critical importance to the railway supply industry and the Nation. My name is Mike O'Malley and I serve as president of the Railway Supply Institute (RSI), an international trade association representing more than 200 companies involved in the manufacture or delivery of goods and services in the locomotive, freight railcar, maintenance of way, communications and signaling, and passenger rail industries. RSI members provide critical products to Class I and short line railroads, shippers, Amtrak, and commuter and transit authorities nationwide. We work with these customers to create new products or services that drive enhancements in both safety and efficiency across their rail networks.

### Introduction

The rail system of the United States is one of our country's greatest assets, covering more than 140,000 miles and carrying 40 percent of America's intercity freight, including 111 million tons of hazardous materials. It also transports millions of passengers every day—from small transit systems to large commuter authorities to intercity service provided by Amtrak or other entities. These systems are supported by an extensive, domestic railway supply industry that has been a dynamic and vital part of the U.S. economy for over 200 years, encompassing 125,000 jobs across all 50 States and paying an average wage 40 percent higher than the national average.<sup>1</sup> Without this robust domestic rail supply industry, our Nation's passenger and freight railroads simply could not meet their customers' needs.

Unfortunately, over the past decade our industry has witnessed substantial intervention in the global rail marketplace from nonmarket economy foreign Governments. Most notably, the People's Republic of China—working through State-owned enterprises (SOEs) like CRRC—has identified rail manufacturing as a strategic market sector and made clear their intention to “conquer” the global rolling stock market.<sup>2</sup> Backed by the full resources of the Chinese Government, CRRC and its affiliates have leveraged direct subsidies, State-backed financing, and below-market loans to secure more than \$2.6 billion in railcar contracts at far below market rate for transit agencies in Boston, Chicago, Los Angeles, and Philadelphia. These manipulative incursions into the U.S. market present both national and economic security risks. There is ample evidence illustrating the Chinese Government's willingness to use industrial espionage, hacking, intellectual property theft, and more to achieve its global objectives, giving us every reason to be concerned about their involvement with critical rail infrastructure and the technology that supports it.

Thankfully, Congress has recognized this threat and begun taking proactive efforts to address it. In a time when consensus on major issues facing the Nation seems as difficult as ever, both houses of Congress and the President united on a bipartisan basis to take strong, proactive action last year to address this threat. But the threat remains, so it is critical that Congress and the Administration continue to scrutinize CRRC's unfair practices, ensure that the Transportation Infrastructure Vehicle Security Act (TIVSA) is implemented quickly as intended, and enact future policies that will discourage CRRC from further undermining the U.S. railcar manufacturing market. For example, this Committee can help ensure that Congress approves a long-term infrastructure bill that gives passenger rail agencies—and the suppliers that support them—the resources they need to make sustainable investments right here in the United States. Members of this Committee have undoubtedly been given a whole host of reasons why an infrastructure bill is important to our future, but I would like to offer one more—American rail supply manufacturers absolutely depend on it. The best way to encourage investment in American jobs and rolling stock manufacturing is to increase investments in passenger rail and provide the certainty associated with a long-term bill.

My goal with this testimony is to provide a comprehensive picture of CRRC's targeting of the U.S. rail market, discuss the industry's outlook moving forward, and to offer policy recommendations that would further enhance the economic and national security of U.S. rail infrastructure against foreign Government interests.

### Chinese SOEs Present an Imminent Threat to the Global Rail Industry

CRRC is the product of a State-directed merger in 2014 between China's two largest State-owned rail companies, China South Locomotive & Rolling Stock Corporation (CSR) and China North Locomotive & Rolling Stock Corporation (CNR). That

<sup>1</sup>“Tracking the Power of Rail Supply, The Economic Impact of Railway Suppliers in the U.S.”, <https://www.rsweb.org/Files/EIS%202018/RSI-Infographic%20FINAL.pdf>

<sup>2</sup>@CRRC-global, “Following CRRC's entry to Jamaica, our products are now offered to 104 countries and regions. So far, 83 percent 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 percent?” Twitter, January 11, 2018.

merger, coupled with hundreds of millions of dollars in support from the Chinese Government, has allowed CRRC to quickly establish itself as the largest producer of rail rolling stock in the world. In 2018, CRRC claimed to have over 180,000 employees with revenues exceeding \$37 billion USD,<sup>3</sup> more than that of its three largest competitors combined. As an SOE, CRRC benefits from the full resources of the Chinese Government and has been repeatedly used to spearhead political initiatives driven by the Chinese Communist Party (CCP). The “Made in China 2025” plan explicitly lists rail as one of ten sectors that China is targeting for global domination over the next 5 years. Similarly, CRRC has been at the forefront of the Belt and Road Initiative, receiving virtually unlimited support from the Chinese Government to finance strategic rail infrastructure projects across the globe.

All evidence suggests that CRRC is driven by these national policy objectives, not market principles, making it impossible for other companies to compete on a level playing field. In fact, CRRC’s own bylaws explicitly direct the company to seek guidance from the CCP on significant matters affecting the company’s operations.<sup>4</sup> The company has also demonstrated a history of intellectual property theft and serious questions have been raised about its labor practices. As a 2017 U.S.–China Economic and Security Review Commission report noted, CRRC’s predecessor companies forced technology transfer agreements on many of the world’s leading rail companies, which Chinese engineers then adapted through a process China has termed “digestion and re-innovation.”<sup>5</sup> A recent NBC news report also linked CRRC to the use of child labor in Madagascar—producing component parts for the same railcars it is now assembling in the United States.<sup>6</sup>

In recent years, CRRC’s pattern of underbidding has become one of our industry’s greatest challenges. Since 2014, CRRC and its affiliates have leveraged State-backed financing and below-market loan rates to secure more than \$2.6 billion in railcar contracts for transit agencies in Boston, Chicago, Los Angeles, and Philadelphia. The company has won these contracts by as much as 30 percent below the next lowest bid, suggesting that these are hardly market-based offerings and that they would not be possible without the support of massive subsidies from the Chinese Government.

Emboldened by winning those contracts, CRRC moved on to target America’s largest and most security-sensitive cities as well. In March 2018, the Metropolitan Transit Authority (MTA) of New York announced that CRRC was among the winners of a “Genius Grant Transit Challenge”, which challenged companies to develop innovative solutions to improve New York City’s subway system. Despite the absence of any ongoing procurements, CRRC committed to invest \$50 million of its own funds to develop the city’s next generation subway car, prompting 15 bipartisan members of the New York congressional delegation to raise concerns with the MTA directly.<sup>7</sup> Here in Washington, D.C., CRRC announced its intent to bid on the Washington Metropolitan Transit Authority’s (WMATA) ongoing rolling stock procurement, prompting members of Congress, including two who serve on this Committee, to once again raise concerns directly with WMATA.<sup>8</sup> These concerns that were echoed again just last month by Secretary of State Mike Pompeo in an address before the National Governors Association.<sup>9</sup>

These concerns are certainly warranted. National security experts have consistently raised the alarm about the ability of CRRC to leverage the technologies on these railcars for espionage or other illicit activities.<sup>10</sup> Many of these trains will contain or interact with Wi-Fi systems, automatic train control, automatic passenger counters, surveillance cameras, and other Internet of Things (IoT) technology that are thoroughly integrated into the information and communications technology in-

<sup>3</sup> CRRC Company Profile, <https://www.crrec.cc/g5141.aspx>.

<sup>4</sup> “CRRC Corporation Limited Articles of Association”, CRRC Corporation Limited, at 70. <http://www.crrec.cc/Portals/73/Uploads/Files/2018/6-4/636637164457871915.pdf>

<sup>5</sup> U.S.–China Economic and Security Review Commission, “China’s High Speed Rail Diplomacy”, February 21, 2017. <https://www.uscc.gov/sites/default/files/Research/China's%20High%20Speed%20Rail%20Diplomacy.pdf>

<sup>6</sup> NBC News, “Zone Rouge: An Army of Children Toils in African Mines”, November 18, 2019. <https://www.nbcnews.com/news/all/army-children-toil-african-mica-mines-n1082916>

<sup>7</sup> Letter to Metropolitan Transit Authority, May 21, 2019. <https://kathleenrice.house.gov/uploadedfiles/20190521-mtaletter.pdf>

<sup>8</sup> Letter to Washington Metropolitan Transit Authority, January 18, 2019. <https://www.scribd.com/document/397856431/WMATA-Cyber-Concerns-8000-Series-Rail-Car-RFP>

<sup>9</sup> Secretary Pompeo remarks to National Governors Association 2020 Winter Meeting, February 8, 2020. <https://www.youtube.com/watch?v=g1BbswU3i10>

<sup>10</sup> *The Hill*, “Opinion—Defense Bill Must Protect U.S. Rail System Against Chinese Cyberintrusions”, David N. Senty and Mark S. Sparkman, 2 October 2019. <https://thehill.com/opinion/cybersecurity/463704-defense-bill-must-protect-us-rail-system-against-chinese-cyber>

infrastructure of transit authorities, all designed and built by a company controlled by the CCP and the Government of China.

### **CRRC a Threat to U.S. Jobs and Economic Security**

Unlike its competitors, CRRC has established assembly operations—not traditional manufacturing operations—to complete these contracts, hiring far fewer employees than comparable plants run by railcar manufacturers that have heavily invested here in America for decades. CRRC constructs the cars in China and then ships them to the U.S. for final assembly. As a result, U.S. components and labor are far more limited than those utilized by their competitors. By contrast, most of the other major rolling stock manufacturers here in the United States source the vast majority of their components domestically, often significantly exceeding minimum Buy America requirements.

To date CRRC has established two assembly facilities in Springfield, MA, and Chicago, IL, and based on media reports these facilities have just 200 employees in total.<sup>11</sup> This illustrates the clear distinction between the type of American manufacturing that Federal and State passenger rail investments are designed to produce and assembly operations of the CRRC. To be clear, we do understand the value those jobs bring to their communities, but the fact is that they came at a cost. A study from *Oxford Economics* estimated that for every job CRRC creates here in the United States to assemble passenger railcars, between three and five jobs are eliminated elsewhere in the domestic supply chain.<sup>12</sup> Oxford estimated that this could result in the loss of as many as 5,100 U.S. jobs and \$330 million in GDP in the passenger railcar market alone if action was not taken. It is not a coincidence that passenger railcar manufacturing plants near Chicago and in Philadelphia closed in recent years after their local authorities awarded contracts to CRRC.

### **Evidence That CRRC Intends To Use Passenger Rail as a Foray Into Freight Manufacturing**

Equally concerning is the prospect of CRRC utilizing its existing beachhead in passenger railcar assembly to move into the freight rail sector. There they could build freight railcars used to transport sensitive military equipment, hazardous materials, critical commodities, and more. As many former military and intelligence officials have repeatedly noted, there are substantial risks in allowing a Chinese SOE to build, operate, or otherwise involve itself in the manufacture or assembly of those freight railcars. During times of war, the U.S. rail network is critical to our military's ability to deploy assets quickly and decisively. Other witnesses for this hearing will provide more detail on this subject, but given these strategic threats and China's growing military capacity, we should take great care in deciding who we rely on for military readiness. As the Department of Defense Office of Industrial Policy noted in a 2018 report, "The decline in the U.S. manufacturing industry creates a variety of risks for America's manufacturing and defense industrial base and, by extension, for DoD's ability to support national defense."<sup>13</sup>

Because freight rail is funded almost entirely with nonpublic funds, there are no Federal content standards as we see in passenger rail, and thus nothing preventing CRRC from aggressively targeting domestic railcar and component manufacturers using nonmarket tactics. CRRC's penetration of the freight market could therefore happen very quickly and with virtually no transparency. This would have a devastating effect on our country's ability to manufacture and deliver freight railcars independently.

The experience of the Australian market serves as perhaps the best example of what can happen in the freight rail sector. In a period of less than 10 years, the Australia's freight railcar manufacturing was rapidly overtaken by CRRC and its predecessor companies as it systematically drove its competition out of the market. Today, there is no meaningful producer of freight rail rolling stock in Australia and thus China is effectively the sole supplier. Independent research has suggested that

<sup>11</sup> *Boston Business Journal*, "Lights Off at CRRC's Springfield Train Car Factory? Company Execs Say It Could Happen", October 10, 2019. <https://www.bizjournals.com/boston/news/2019/10/10/lights-off-at-crrcs-springfield-train-car-factory.html>

<sup>12</sup> *Oxford Economics*, "Assessing How Foreign State-Owned Enterprises' U.S.-Based Operations Disrupt U.S. Jobs", June 2019. <https://www.oxfordeconomics.com/recent-releases/assessing-how-foreign-state-owned-enterprises-us-based-operations-disrupt-us-job>

<sup>13</sup> U.S. Department of Defense, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States", September 2018. <https://media.defense.gov/2018/Oct/05/2002048904/-1/-1/1/assessing-and-strengthening-the-manufacturing-and%20defense-industrial-base-and-supply-chain-resiliency.pdf>

similar actions in the United States could result in the loss of as many as 65,000 U.S. jobs and \$6.5 billion in GDP.<sup>14</sup>

While CRRC has recently claimed they have no interest in the freight segment of the market, their actions show otherwise. In 2014, CRRC entered into a now-defunct joint venture with a Chinese holding company and a U.S. firm to launch Vertex Rail Corporation, a freight railcar assembly facility located in Wilmington, North Carolina. Despite nearly 100 members of the House and Senate raising national security concerns with the investment, it was ultimately allowed to move forward.<sup>15</sup> While that venture closed in November 2018, there is little doubt that the U.S. market remains a prime target. In fact, there are indications that CRRC is already establishing a presence in Canada with the intent to import freight cars into the U.S. market.

### Current Actions and Policy Recommendations

RSI and our members are grateful for the actions policymakers have taken thus far to mitigate CRRC's threat. Beginning with successful efforts to reform the Committee on Foreign Investment in the United States (CFIUS), Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018. This gives future Administrations the tools needed to thoroughly review transactions like those of CRRC and Vertex moving forward and take appropriate steps to block those transactions if they are deemed a threat to national security.

The passage of the Transit Infrastructure Vehicle Security Act (TIVSA) is also an important step forward. This legislation will block any Federal funds from being used to subsidize CRRC's activities in the future, ensuring that CRRC is unable to further leverage American taxpayer funds to underbid its competition. It also institutes much-needed cybersecurity standards that will help limit the national security risks associated with CRRC's existing or future contracts.

These legislative achievements are important steps for the industry, but it is essential that we not get complacent in the wake of China's clear desire to overtake our industry. We offer the following recommendations for policymakers to continue to be proactive in countering this threat:

1. *The Federal Transit Administration (FTA) should immediately communicate with its grantees on TIVSA to ensure compliance with this new law.* We have heard some suggestion that there is confusion regarding what this bill does. To us, lawmakers were clear in passing this legislation that there are significant national and economic security risks associated with awarding a contract to CRRC and that Federal funds should not be used to award a contract to a Chinese SOE. Yet CRRC has said that it will continue to aggressively bid on contracts.<sup>16</sup> As leaders of this Committee have so clearly articulated, it is essential that the FTA communicate to transit agencies to ensure prompt compliance with Congress' intent in passing this legislation as part of the National Defense Authorization Act.

2. *Congress should pass a long-term infrastructure bill with robust passenger rail funding levels to ensure that States and localities can make smart, sustainable investments for the future.* CRRC's success in winning Federal and State transit contracts has been fueled by their ability to come in at below-market prices by leveraging Government subsidies, under procurement rules that often require transit agencies to award contracts to the lowest bidder. People are increasingly recognizing the benefits of passenger rail and States and localities are making rolling stock investments to support it, but predictable, dedicated and sustainable sources of Federal funding are needed.

3. *Pass legislation or direct the U.S. Department of Transportation to ensure strict Buy America compliance, spurring domestic jobs and limiting the ability of foreign SOEs to game the system.* By design, Buy America laws were written to ensure that taxpayer dollars made available for constructing and sustaining our public transportation systems would flow back into the U.S. economy and discourage the outsourcing of these manufacturing jobs to other countries. Unfortunately, RSI believes that the U.S. Department of Transportation currently lacks adequate resources to ensure strict compliance with Buy America provisions across the country. Congress should direct USDOT to exercise stricter oversight to help keep grant funding in the United

<sup>14</sup> Oxford Economics, "Will We Derailed U.S. Freight Rolling Stock Production?", May 2017, at 24. <https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production>

<sup>15</sup> Letter to U.S. Department of Treasury, July 15, 2016. <https://lipinski.house.gov/uploads/CFIUS%20Letter%20to%20Treasury.pdf>

<sup>16</sup> New England Public Radio, "Capitol Hill Deal Keeps Springfield's CRRC Rail Car Factory Rolling", Dec. 12, 2019. <https://www.nepr.net/post/capitol-hill-deal-keeps-springfields-crrc-rail-car-factory-rolling#stream/0>



States and spur the domestic jobs critical to maintaining a strong American manufacturing base.

4. *Create additional safeguards for the freight industry.* While TIVSA was a vital step forward that will help level the playing field in the domestic passenger railcar market, the freight sector remains at risk. RSI will be working this year with members of Congress to identify legislation that could help establish appropriate standards for freight railcar manufacturing so we can ensure that CRRC does not wipe out the market in the same way they did in Australia. Given actions already taken by CRRC and the criticality of freight rail networks for national security and military deployment capabilities, we must act quickly.

I will make one final point. Given the global nature of this threat, many of our allies are now following the lead of U.S. policymakers to address the issue in other markets as well. In Europe, for example, the European Commission is actively exploring ways to address the threat. The Association of the European Rail Supply Industry (UNIFE) recently issued a call to action given the expansion of China's State-owned rail suppliers, citing "the threat to European rail suppliers and the 400,000 jobs they represent due to unequal competition and State subsidies to Chinese players."<sup>17</sup> We encourage the U.S. Congress and Administration to work with our allies across the globe to unite in the effort to ensure a market-driven railway supply sector free from SOE interference.

### Conclusion

RSI members will continue investing and doing all we can to support our passenger agency customers in serving the mobility and economic development needs of communities across the country, but we cannot compete with an entire country in a marketplace distorted by Chinese Government subsidies. We appreciate the opportunity to provide these recommendations on critical issues affecting our industry and will continue working with members of Congress to formulate policies that enhance rail safety, security, and efficiency. Thank you for the opportunity to testify and I would be happy to answer any questions that you may have.

---

### PREPARED STATEMENT OF SCOTT N. PAUL PRESIDENT, ALLIANCE FOR AMERICAN MANUFACTURING

MARCH 5, 2020

Chairman Crapo, Ranking Member Brown, and Members of the Committee, on behalf of the Alliance for American Manufacturing (AAM), thank you for the opportunity to testify at today's hearing on the Threats Posed by State-Owned and State-Supported Enterprises to Public Transportation.

The Alliance for American Manufacturing is a nonprofit, nonpartisan partnership formed in 2007 by some of America's leading manufacturers and the United Steelworkers. Our mission is to strengthen American manufacturing and create new private-sector jobs through smart public policies. We believe that an innovative and growing manufacturing base is vital to America's economic and national security, as well as to providing good jobs for future generations. AAM achieves its mission through research, public education, advocacy, strategic communications, and coalition building around the issues that matter most to America's manufacturers and workers.

### The TIVSA Law Is an Important Milestone

For the last two decades, we have seen the destructive impacts of China's model of State-led capitalism on our domestic manufacturing sector, and the damaging ripple effects on thousands of communities across our Nation. Between 2001, when China entered the World Trade Organization (WTO), and 2018, 3.7 million U.S. jobs were lost or displaced because of our massive bilateral trade deficit with China.<sup>1</sup> This carnage has been fueled by predatory trade practices and disruptive economic policies, including massive subsidization of State-owned enterprises (SOEs) and other "champion" firms that Beijing has deemed strategically important to their own economic and security interests.

More recently, we have witnessed China's State-owned and State-supported rolling stock companies threaten legitimate competition in the markets that serve our

---

<sup>17</sup> UNIFE, "A Call for Urgent Action: The Fast Expansion of China's State-Owned Rail Suppliers", November 2019.

<sup>1</sup> "Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018: Jobs Lost in Every U.S. State and Congressional District", Robert E. Scott and Zane Mokhiber. Economic Policy Institute. 30 January 2020.

public transportation system. Backed by extensive Government support, including Made in China 2025, China Railway Rolling Stock Corporation (CRRC) and Build Your Dreams (BYD) are at the forefront of China's assault. Their penetration into our market has been accelerated by open access to taxpayer-financed railcar and electric bus procurements in major U.S. cities. In other words, these firms have penetrated our market with not only Beijing's backing, but also on the backs of American taxpayers.

China's subsidies and other governmental support allow CRRC and BYD to underbid the competition, but you get what you pay for. The taxpaying public has received dangerous railcars plagued by undercarriage faults, door malfunctions, and derailment and electric buses experiencing brake pressure issues, door issues, cracked and missing welds compromising the integrity of the buses, malfunctioning wheelchair accessibility, and exposed high voltage cables that created a risk of electrical fire.<sup>2</sup>

Left unchecked, the toll on U.S. supply chains will be devastating. Because CRRC and BYD's U.S. assembly operations are a supply line for major rolling stock components produced in China, the jobs of American workers throughout our domestic supply chains are now at risk. A recent *MassLive* article describes the business model well: "[CRRC's] cars come to Springfield as unfinished metal shells built in China. Here, workers install all the electronics, interiors, motors and other equipment."<sup>3</sup> Meanwhile, a city official familiar with BYD's assembly operations remarked that "the majority, if not all, parts were manufactured in China and shipped to the United States."<sup>4</sup>

China's ambitions are sizeable: To establish a substantial foothold into our public transit market as a means of expanding into private sectors such as the freight rail and electric vehicle markets. Jobs, supply chains, innovation, and the security of Americans using our public transportation systems are all at risk. We are also deeply concerned about China's "military-civil fusion" partnerships, which means that doing business with China's State-owned and State-supported enterprises directly finances China's development of its military capabilities and proliferation of its surveillance regime. Technology and data obtained by these firms in the United States is handed directly to the Chinese military and each collaborates with Huawei.

We are grateful that Congress—under your bipartisan leadership—has begun taking action to mitigate this threat. As China's State-backed firms have sought to avail themselves of U.S. tax dollars to advance Beijing's broader economic and military interests, your bipartisan leadership led to passage of a version of the Transportation Infrastructure Vehicle Security Act (TIVSA) as part of the fiscal year 2020 National Defense Authorization Act (NDAA). If TIVSA is properly implemented as intended by Congress, CRRC and BYD will no longer have unfettered access to the Federal dollars used to procure public transit vehicles. The TIVSA law represents an important milestone in the United States' policy response to the threat of China's State-driven gaming of our economy.

Yet, China's assault on our public transportation infrastructure is not likely to subside and the manufacturing capabilities that underpin America's public transportation remain at risk. It is necessary for Congress to remain vigilant about the threat that China's State-owned and State-supported firms continue to pose to American jobs, supply chains and national security:

- We must ensure that the Administration implements the TIVSA law without delay and as Congress intended.
- We must reject shortsighted attempts to undermine the TIVSA law.
- We must be better stewards of U.S. tax dollars by closing loopholes and ensuring compliance with applicable Buy America laws.
- We must incentivize the production of electric vehicle batteries and battery cells in the United States.
- And, we must invest in America's failing infrastructure.

AAM has a long history of standing up to China's cheating on trade policy, including its environmental and labor record. For 12 years we have worked with leaders of both parties to push back against dumping, subsidies, currency manipulation, and other unfair trade practices that have cost millions of American workers their jobs over the past two decades. It is unfortunate that some have chosen to attack us for

<sup>2</sup>"Inspection of Albuquerque Rapid Transit Project Procurement", Peter Pacheco, Office of the Inspector General, City of Albuquerque. 6 June 2018.

<sup>3</sup>"Rail Car Maker CRRC MA Deals With Production Delay, Trade Tensions as It Builds Warehouse for East Springfield Factory", Jim Kinney. *MassLive*. 9 February 2020.

<sup>4</sup>"Inspection of Albuquerque Rapid Transit Project Procurement", Peter Pacheco, Office of the Inspector General, City of Albuquerque. 6 June 2018.

offering fact-based information to policymakers. To date, neither BYD nor CRRC have refuted any facts that AAM or others have laid out about their deep connections to the Chinese Government, the Communist Party, the Chinese military, or other State-championed firms like Huawei.

It is the duty of this Committee and of Congress to scrutinize how these firms are systematically seeking to destroy the competitive national landscape for U.S. rolling stock manufacturing. We must strive to be good stewards of American tax dollars and promote a competitive, market-based ecosystem of companies that do not benefit from aggressive foreign Government support to bankroll anticompetitive behavior.

Again, thank you for the opportunity to testify at today's hearing. My full testimony has detailed information on CRRC and BYD, along with policy recommendations that we hope you will take into consideration.

### **China Railway Rolling Stock Corporation (CRRC)**

#### *CRRC Threatens U.S. Rail Supply Chains*

In 2014 the Massachusetts Bay Transportation Authority (MBTA) made what we believed to be a shortsighted decision to award a \$566 million railcar contract to a Chinese SOE, CNR, that would soon after become CRRC after merging with yet another Chinese State-owned rolling stock firm that was disqualified from the same bidding process. CRRC's bid was more than \$200 million below the next lowest bidder and roughly half that of another established firm. At the time, I wrote to then-Massachusetts Governor Deval Patrick warning that granting this award with tax dollars would reward and enable illicit competition tied to the Chinese Government. "As a basic principle of fairness, all bids should play by the same set of market rules and none should be allowed to benefit from the backing of a foreign Government. It is cheating, plain and simple, and should not be rewarded using taxpayer dollars," I wrote. "By making [CRRC's] entry into the U.S. market possible, this procurement opens the door to unfair, State-owned competition on other rail and transit procurements throughout the United States."

Regrettably, AAM's warning was ignored, and the concerns outlined in that letter more than 5 years ago have become reality. Once MBTA legitimized CRRC with its first major U.S. transit contract, it quickly secured an additional \$2 billion in transit railcar contracts in Philadelphia, Los Angeles, and Chicago with low bids that no private-sector competitor could possibly match. In Philadelphia, a competitor was quoted as saying, "I cannot grasp how they are able to do it at that cost."<sup>5</sup> Compounding the damage, MBTA granted another \$277 billion contract to CRRC 2 years later.

With the financial backing of Beijing, CRRC is systematically working to drive established competitors out of the market and achieve a monopoly in U.S. and global railcar production. But, don't just take my word for it. In January of 2018, CRRC tweeted, "Following CRRC's entry to Jamaica, our products are now offered to 104 countries and regions. So far, 83 percent 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 percent?"<sup>6</sup> This tweet was later deleted.

We acknowledge that Boston, Los Angeles, and Chicago secured commitments that final assembly of CRRC railcars be completed locally with additional pledges of support for local workers. That these transit agencies sought to preserve some American jobs is commendable, but their efforts do little to mitigate other overwhelmingly negative impacts to our Nation. High-wage jobs throughout the U.S. rail manufacturing supply chain are at risk of being displaced by workers operating under harsh conditions and little pay in China. CRRC's U.S. assembly plants are a vehicle—both literally and figuratively—for Chinese content to be delivered into the U.S. market.

As of 2015, there were more than 750 companies in at least 39 States that manufacture components for passenger rail and transit rail. This includes: 24 major locomotive, railcar, and streetcar assembly facilities; 188 direct suppliers that manufacture major propulsion, electronics, and body components and systems; and, in the Midwest and Mid-Atlantic alone, 540 additional companies manufacturing sub-components, materials, track and infrastructure, as well as providing repair and re-manufacturing to the industry. All told, the U.S. rail manufacturing sector supports

<sup>5</sup>"Mass.-Based Company With Chinese Backing Beats Local Group for SEPTA Car Contract", *The Philadelphia Inquirer*. 21 March 2017.

<sup>6</sup>@CRRC—Global, "Following CRRC's entry to Jamaica, our products are now offered to 104 countries and regions. So far, 83 percent 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 percent?" Twitter, January 11, 2018. [Tweet deleted]

90,000 jobs.<sup>7</sup> As noted earlier in my testimony, CRRC's entry into the U.S. transit procurement market is almost assuredly a precursor to penetrating our freight rail market, a sector that not only supports 65,000 manufacturing jobs but is also responsible for moving 40 percent of all goods in the United States.<sup>8</sup>

#### *Quality and Safety of CRRC Railcars Is a Recurring Issue*

In only a limited period, there are already numerous accounts of quality and safety problems with CRRC railcars carrying passengers in Boston. Just this week, MBTA removed CRRC railcars from service after identifying a serious equipment fault. According to authorities, "Inspectors identified a fault with the bolsters which is being corrected to ensure the vehicles are reliable and safe . . ." <sup>9</sup> <sup>10</sup> According to an MBTA spokeswoman, the bolster is a beam underneath the railcar that allows navigation along turns on the track. This news is even more concerning given that it is third time CRRC railcars have been pulled from this particular train line since delivery. In December 2019, CRRC railcars witnessed odd noise related to a different undercarriage problem and, in September 2019, a malfunction opened doors while the trains were in motion.<sup>11</sup> Worse yet, a CRRC train derailed from its tracks in November 2019.<sup>12</sup>

#### *CRRC Poses a Serious Security Threat*

CRRC's rapid ascent raises alarming questions about Beijing's backdoor access to and operational control over critical technology embedded in our rail infrastructure—such as GPS, sensors and other safety features. Within the TIVSA law, policymakers rejected the possibility that the Washington Metropolitan Area Transit Authority (WMATA) could award its pending procurement for its 8000-series railcar to CRRC. This was a clear statement that Beijing should not have operational control of or access to a major U.S. transit system, opening our critical infrastructure to potential attack or backdoor access to sensitive data and communications of riders. Putting railcars manufactured by a Chinese State-owned firm underneath the Pentagon in Washington, D.C., or near sensitive locations in New York City or anywhere else in America is a horrible idea.

As you will hear from other experts on today's panel, CRRC is Beijing's national champion in rail and emerging transportation systems. It plays a direct role in China's military-civil fusion strategy. According to research released by Radarlock in 2019, CRRC is working directly with Beijing to obtain foreign technology, collect sensitive data, and export technologies and information systems that threaten individual and data security, including those of Huawei. CRRC executives wear "dual hats" as corporate and Party leaders, appointed for political purposes.<sup>13</sup>

#### **Build Your Dreams (BYD)**

##### *BYD Wants To Move From Electric Buses to Electric Automobiles in the United States*

In 2013 BYD, short for "Build Your Dreams", established an electric bus assembly facility in Lancaster, California, signaling its intention to compete for taxpayer-funded transit contracts in U.S. cities. BYD says it has more than 50 public and private customers in the United States, including universities and airports, and has delivered more than 400 electric buses from its California facility. Globally, it claims to have 40,000 electric buses in service<sup>14</sup> and is a major producer of rechargeable battery technology in China for various end products.

Like CRRC, BYD's unparalleled State-subsidies and low-cost, State-backed supply chain of imported Chinese parts and components allow it to undercut competition with impossibly low prices. A recent San Francisco pilot purchase of three electric buses each from BYD and two competitors showed that the Chinese State-supported

<sup>7</sup>"Passenger Rail & Transit Rail Manufacturing in the U.S.", BlueGreen Alliance and the Environmental Law & Policy Center. January 2015.

<sup>8</sup>"Will We Derailed U.S. Freight Rolling Stock Production: An Assessment of the Impact of Foreign State-Owned Enterprises on U.S. Freight Rolling Stock Production", *Oxford Economics*, May 2017.

<sup>9</sup>"MBTA Taking New Orange Line Trains Out of Service", Emily Sweeney. *Boston Globe*. 3 March 2020.

<sup>10</sup>"MBTA Takes All New Orange Line Trains Out of Service for Repair", Stefan Geller. *Boston Herald*. 3 March 2020.

<sup>11</sup>"CRRC: The MBTA Is Handling Latest Problem With Springfield-Built Orange Line Cars", Jim Kinney. *MassLive*. 3 March 2020.

<sup>12</sup>"MBTA Investigating Derailment of New Orange Line Train in Medford Rail Yard", Steph Solis. *MassLive*. 18 November 2019.

<sup>13</sup>"CRRC and Beijing's Dash for Global Rolling Stock Dominance", Bruyere and Picarsic. *Radarlock*. October 2019.

<sup>14</sup>BYD website.

firm's price tag came in millions of dollars below the established, market-driven competition.<sup>15</sup>

Already one of the world's largest battery producers and the world's largest electric vehicle company, BYD executives have been outspoken in their plans to one day sell passenger electric vehicles in the United States. In 2008, BYD's chairman has "boasted of plans to dominate world auto sales by 2025" and, more recently, a BYD executive said the company planned to sell passenger cars in the United States in "roughly 2 to 3 years." Left unchecked, BYD's business model would threaten over 5,600 auto parts suppliers spread across the Nation, employing 871,000 workers.<sup>16</sup>

#### *BYD Buses Plagued by Quality and Safety Concerns*

BYD's struggles with quality, consistency, and performance have been well documented. According to Albuquerque officials, bus batteries limited the bus range to 177 miles on a single charge, far short of the 275 miles stipulated in its contract. The buses also experienced serious safety issues, including brake pressure issues, door issues, cracked and missing welds compromising the integrity of the buses, malfunctioning wheelchair accessibility, and exposed high voltage cables that created a risk of electrical fire.<sup>17</sup> The city has resorted to legal action against BYD.<sup>18</sup>

Meanwhile, Los Angeles city transit agency staff "called them 'unsuitable,' poorly made and unreliable for more than 100 miles," the *LA Times* reported. Buses used in Los Angeles experienced white smoke from a rear wheel, wouldn't start on a second run, lost charge after just 68 miles, and stalled on the road. Others serving Disney resorts experienced door and air system failures. In Denver, bus doors would not open or close. In Columbia, Maryland, passengers were "jolted by an explosion and a wheel fire."<sup>19</sup>

#### *BYD Is a National Champion of China's Electric Battery Goals*

While BYD is not a "State-owned" company in the same advertised manner as CRRC, it enjoys many of the same benefits and has similar connections to Communist Party Leaders, the China's military, and firms like Huawei. As the U.S.-China Economic & Security Review Commission has noted, "some private Chinese companies operating in strategic sectors are private only in name, with the Chinese Government using an array of measures, including financial support and other incentives, as well as coercion, to influence private business decisions and achieve State goals."<sup>20</sup>

The Made in China 2025 strategy identified new energy vehicles as one of ten priority sectors for developing indigenous innovation capability, making the sector a priority, high-technology industry important to China's mid- and long-term growth strategy. BYD is one of China's "national champions" meaning Beijing believes it has a high potential for growth, innovation, and the ability to advance China's industrial and other policy goals. "At the heart of BYD's technology is its batteries for a broad range of applications—from cell phones and laptops to large-scale, grid-connected energy storage systems," its website boasts.<sup>21</sup> There are documented cases of BYD's battery technology being provided to China's military.<sup>22</sup>

As a national champion, BYD has been the beneficiary of a mix of Government support, including a lower corporate tax rate in China, loans from State-owned and policy banks, and generous grants and subsidies. China initiated its Government support for new energy vehicles in 2009 targeting battery, hybrid, and fuel cell electric vehicles, including both passenger and commercial vehicles.<sup>23</sup> This support grew over time and, according to a 2019 *Bloomberg* article, "the company received new energy vehicle subsidies equal to 380 percent of its electric car sales . . . [getting] about 8.2 billion yuan (\$1.2 billion) from the central Government and 4.4 bil-

<sup>15</sup>"Transit Agency Approves Pilot Contracts To Test Electric Buses", Jerold Chinn. SFBay.ca. Website. 6 November 2019. Accessed 29 Feb 2020.

<sup>16</sup>"State of the U.S. Automotive Industry", American Auto Policy Council. August 2018.

<sup>17</sup>"BYD Faces Albuquerque Lawsuit: City Claims Bus Firm Didn't Live up to Deal", *Antelope Valley Press*. 08 December 2018.

<sup>18</sup>City of Albuquerque v. BYD Motors, Inc., No. 1:2019-cv-00012 (U.S. Dist. Ct., NM).

<sup>19</sup>"Stalls, Stops and Breakdowns: Problems Plague Push for Electric Buses", Paige St. John. *Los Angeles Times*. 20 May 2018.

<sup>20</sup>U.S.-China Economic and Security Review Commission, 2017 Annual Report to Congress, at 3.

<sup>21</sup>"About", BYD website.

<sup>22</sup>"Building the China Dream: BYD & China's Grand Strategic Offensive", Bruyere and Picaresc. Radarlock. October 2019.

<sup>23</sup>Compiled from Government of China Announcements.

lion yuan [\$647 million] from local governments.” This Government backing made it possible for BYD to deploy its battery technology into commercial vehicles.<sup>24</sup>

#### *BYD Is Closely Aligned With Beijing*

While BYD consistently cites Warren Buffett as its largest shareholder, there are several Chinese State-owned investment funds that hold equity interests in BYD or its subsidiaries.<sup>25</sup> Meanwhile, BYD’s leadership have past and present ties to local and national Chinese Governments. For instance, BYD’s Chairman and CEO Wang Chuanfu owns a significant stake in the company and was a delegate of the People’s Congress of Shenzhen from 2000 to 2010 and held a position with the city legislature from 2005 to 2015.<sup>26</sup> Much of BYD’s staggering global growth is owed to BYD’s nearly exclusive access to its home market of Shenzhen, a city of twelve million people, where it supplied upwards of 80 percent of the city’s 14,000 electric buses.<sup>27</sup> Zou Fei, an expert of the “Thousand Talents Program” of the Central Committee of the Communist Party of China,<sup>28</sup> was previous managing director within the sovereign wealth fund responsible for managing China’s foreign exchange reserves. Also the deputy general manager of Norinco Group—a State-owned defense company—serves as a supervisor on BYD’s Board.<sup>29</sup>

Despite its best efforts to brand itself as a private company free of Beijing’s influence, BYD’s direct and active role in China’s military–civil fusion strategy is deeply disturbing and well documented in the 2019 Radarlock Report, “Building the China Dream: BYD & China’s Grand Strategic Offensive”. BYD uses its status as a “private company” to “obtain technology, information, and positioning from the international market, then to carry those back to the CCP and the People’s Liberation Army (PLA).” Meanwhile, its research and development centers are “incubated” in military–civil fusion zones that focus on technology transfer and data sharing. BYD and now-banned Huawei signed a “comprehensive strategic cooperation agreement” in March 2019, solidifying a long-standing, “inseparable” partnership between the two firms. BYD not only benefits from the Made in China 2025 strategy, it is helping to formulate the next iteration: China Standards 2035.<sup>30</sup> This paints a troubling profile of a company with deep ties to the Chinese Government and military that is trying to masquerade as a commercial entity.

#### *BYD’s Reliance on Chinese Imports Raises Buy America Compliance Questions*

U.S. domestic content preference laws—including the Buy America law applied to transit Federal assistance—are an important policy to incentivize domestic capital investment and ensure that American workers supply the materials and components used to build our vehicles and infrastructure. An Albuquerque Inspector General report raised significant questions as to BYD’s Buy America compliance and the degree to which it relies on imported Chinese components and parts for the electric buses it assembles in Lancaster, California. While a BYD official said that “only the frames of the buses were made in China,” the IG report offers sharply different accounts from city inspectors. One person interviewed said that “the majority, if not all, parts were manufactured in China and shipped to the United States.” Another observed that “many of the shipping labels for various components had Chinese characters.” After asking about the status of certain components, including lights and seating, an inspector was told “it’s on the boat” and believed that “everything” originated in China based on responses to questions.<sup>31</sup>

A closer look at BYD’s Buy America compliance calculations in the IG report reveal even more alarming questions, particularly with the way battery power systems consisting of Chinese content are counted.

- BYD met the 65 percent statutory threshold<sup>32</sup> with 53 percent of the total cost of materials attributed to its Power Battery System. Meanwhile, import records show that BYD imports massive quantities of battery equipment, including bat-

<sup>24</sup> “Buffett’s China Ride Is Losing Power With Investors”, *Bloomberg*. 19 February 2019.

<sup>25</sup> BYD 2017 Annual Report and BYD Financial Releases.

<sup>26</sup> BYD 2017 Annual Report.

<sup>27</sup> “100% Electric Bus Fleet For Shenzhen (Population 11.9 Million) By End of 2017”, *Clean Technica*. 12 November 2017.

<sup>28</sup> BYD 2017 Annual Report.

<sup>29</sup> BYD 2013 Interim Report.

<sup>30</sup> “Building the China Dream: BYD & China’s Grand Strategic Offensive”, Bruyere and Picarsic. Radarlock. October 2019.

<sup>31</sup> “Inspection of Albuquerque Rapid Transit Project Procurement”, Peter Pacheco, Office of the Inspector General, City of Albuquerque. 6 June 2018.

<sup>32</sup> The statutory Buy America law for rolling stock procurements funded with Federal Transit Administration (FTA) grants requires that assembly occur in the United States and that domestic content account for a minimum of 65 percent as measured by total material cost, increasing to 70 percent by FY2020.

tery cells, from another BYD subsidiary in China. This foreign content is used to assemble a battery pack that ostensibly qualifies as domestic component for purposes of FTA's Buy America regulation.<sup>33</sup> This, in turn, means that all other domestic-origin components—such as seats and the farebox—accounted for as little as 18 percent of the total cost of materials in a BYD electric bus.

- An individual interviewed in the Albuquerque IG report indicated that he felt “pressured” to validate [Buy America] compliance by signing documents representing that he personally validated the origination of the components. Upon being told that “signing the document was just a ‘formality’ to ensure compliance,” he said that he felt “uncomfortable” signing. He later told the IG “that he felt he was under duress in being pressured to sign the document.”
- Meanwhile, the IG report indicates that BYD provided the “summary of calculations for the percentages of United States made parts” to the auditor tasked with ensuring Buy America compliance. Given that many of BYD's imported components and parts come from other divisions of BYD, this raises serious questions as to the validity of that information and how thorough of an audit was conducted.
- As further evidence, we direct your attention to BYD's public comments submitted to the U.S. Trade Representative (USTR) requesting Section 301 tariff relief for storage batteries,<sup>34</sup> air conditioning machines, seats, parts and accessories,<sup>35</sup> and electric vehicles, specifically noting its K9S,<sup>36</sup> K9MC,<sup>37</sup> K7M,<sup>38</sup> and K8S<sup>39</sup> electric bus models. USTR's General Counsel stated that the “request was denied because the request concerns a product strategically important or related to ‘Made in China 2025’ or other Chinese industrial programs.”

#### Policy Recommendations

AAM appreciates your leadership in securing enactment of the TIVSA law. Yet, China's assault on our public transportation infrastructure is not likely to subside and the manufacturing capabilities that underpin America's public transportation remain at risk. There is more work that must be done to mitigate the threat of Chinese State-owned and State-supported companies.

- *Implement TIVSA Without Further Delay.* More than 2 months have now passed since TIVSA enactment and the Administration has yet to notify or release guidance to transit agencies. We are concerned that failing to educate transit agencies in a timely manner about how TIVSA impacts their planning decisions leaves an opening for deception and misinformation.
- *Defend and Enhance TIVSA.* Already, there are forces at work to undermine TIVSA. Shortly after enactment, CRRC held a “thank you” event at which speakers discussed plans to indefinitely extend the 2-year implementation delay.<sup>40</sup> We urge Congress to reject any attempts to undermine the TIVSA law. Instead, AAM supports efforts to accelerate implementation, educate transit agencies, and enhance the law.
- *Tighten Buy America Laws.* AAM supports making improvements to long-standing Buy America laws by closing loopholes, modernizing rules for battery content, and adding additional teeth to prevent erosion of our supply chains. We find it concerning that companies like BYD are meeting the statutory Buy America threshold with electric batteries assembled domestically almost entirely of foreign content, with little to no domestic processing in the United States. It is appropriate, in our view, to recognize that short-term market limitations exist in battery cell production and create a Buy America framework for

<sup>33</sup> BYD's U.S. Imports Derived from Shipping Manifests, 2017 and 2018 YTD as of Nov. 28, 2018. Obtained from Panjiva, Inc.

<sup>34</sup> BYD America Corp. comments and appendix, Proposed Determination of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, Docket No. USTR-2018-0005, May 14, 2018.

<sup>35</sup> BYD Motors LLC comments, China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, Docket No. USTR-2018-0026, Sept. 6, 2018.

<sup>36</sup> Exclusion Denied, BYD Motors Inc., Electric bus, HTS 8702903100, USTR-2018-0025-7530, Oct. 26, 2018.

<sup>37</sup> Exclusion Denied, BYD Motors Inc., Electric bus, HTS 8702903100, USTR-2018-0025-7528, Oct. 26, 2018.

<sup>38</sup> Exclusion Denied, BYD Motors Inc., Electric bus, HTS 8702903100, USTR-2018-0025-7346, Oct. 25, 2018.

<sup>39</sup> Exclusion Denied, BYD Motors Inc., Electric bus., HTS 8702903100, USTR-2018-0025-7347, Oct. 25, 2018.

<sup>40</sup> “CRRC MA, Rep. Richard Neal Celebrate Victory in Washington; Compromise Allows Rail Car Company To Keep Seeking New Work”, Jim Kinney. *MassLive*. 23 December 2019.

electric batteries that rewards value added by American workers. We must also ensure that other non-battery components and parts continue to be produced in the United States and are not diminished by virtue of the outsized cost of the electric battery.

- *Develop a Policy Framework for Domestic Battery Production.* Faced with a deeply distorted global market, Congress and the Administration should work together to establish a mix of incentives and policies that maximize the utilization of new energy vehicles and expand the supply chain for the domestic production of electric batteries and battery cells.
- *Conduct Buy America Audits.* AAM encourages further scrutiny of both CRRC's and BYD's Buy America certifications to ensure compliance. Both companies appear to rely heavily on imported Chinese content and the Albuquerque IG report raised significant questions as to the legitimacy of BYD's certification.
- *Invest in America's Failing Infrastructure.* Last, but certainly not least, we encourage you to continue the challenging work of passing a substantial infrastructure investment paired with strong Buy America requirements.

### Conclusion

We applaud the Committee for holding today's hearing and for your leadership in securing enactment of the TIVSA law. We look forward to working with you to counter the threats to America's public transportation while strengthening U.S. manufacturing.

---

## PREPARED STATEMENT OF EMILY DE LA BRUYERE

PRINCIPAL, HORIZON ADVISORY

MARCH 5, 2020

Thank you, Chairman Crapo, Ranking Member Brown, and Members of the Committee, for inviting me to testify before the Senate Banking Committee this morning.

CRRC and BYD are vehicles of the Chinese State: They receive significant State subsidies, implement Chinese Communist Party (CCP) international strategy, and directly connect to Beijing's military apparatus. Those are facts. You will hear from other witnesses today about immediate implications for national and economic security; about threats to America's manufacturing industrial base and cybersecurity. I echo their serious concerns.

But I am here to tell you about Beijing's plan, about the strategic vision with which China deploys its champions, in transport and in other foundational networks, and the far-reaching implications of that vision for American security.

CRRC, BYD, and the larger ecosystem of Chinese champions operationalize a long-standing, codified, strategic bid to overtake the United States.<sup>1</sup> As documented in CCP literature, that bid begins by making critical U.S. economic and military infrastructures dependent on Beijing. It ends with CCP control over international networks, standards, and platforms—in other words, CCP control over global movement. This is network hegemony. It establishes its footholds in transportation and manufacturing. It extends into health, agriculture, information, information technology, finance. It spans critical technology, infrastructure, and data. If Beijing succeeds, it will claim global coercive power. It will use that power liberally.

Authoritative Chinese sources are explicit about this ambition. Take, for example, 2018 State Council policy guidelines:

The implementation of China's railway strategy will establish a full domestic and "Belt and Road" network that will extend to neighboring countries and even the world: Air transportation, sea transportation, road transportation, logistics nodes, and urban distribution will all be dominated through the leadership of the railway network.<sup>2</sup>

That narrative is matched by the facts: By the mandates China assigns its State champions, the support with which it deploys them internationally, and the policies directing that support—policies that extend from Made in China 2025 to its new

---

<sup>1</sup> Xi Jinping describes this ambition with a Chinese phrase that translates, roughly, to "overtake around a corner." Based on the action of one car passing another car on a corner, the concept refers, in the geostrategic sense, to leveraging moments of flux to overtake a competitor.

<sup>2</sup> Railway Supply-Side Reforms Reshape the Logistics Market Landscape, Logink Network, November 15, 2018.



successor, China Standards 2035;<sup>3</sup> from the Strategic Emerging Industries Initiative to the Transportation Great Power Strategy.

My testimony will walk through these facts as they relate to BYD, CRRC, and the Chinese strategic approach to the transportation domain. I will begin by detailing the ties linking BYD and CRRC to the Chinese Government and military apparatus. I will then discuss the Chinese Government plans shaping those ties, and their implications for U.S. economic and national security.

The network strategy behind Beijing's actions amplifies the first-order risks elaborated by the other witnesses here today. The network power that Beijing has already cemented underscores the immediacy of the threat. China's offensive is underway.

### State and Military Ties

Beijing aggressively subsidizes its transportation champions so that they can underprice international competitors. This tactic may produce a short-term loss. But China is directing its State champions according to a long-term vision: As they capture critical nodes, networks, and supply chains, Beijing more than recoups its investment—both strategically and economically. At a first level, basic American infrastructure systems, systems that Beijing qualifies as national defense structures, come to rely on Chinese actors. At the next, Beijing seizes the information and physical foundations for a new generation of “smart,” or “connected,” infrastructure. Beijing locks in not just asymmetrical dependence, but also information dominance and standard-setting power.

China's intentions are not benign. This approach is part and parcel of Beijing's military agenda, operationalized in a national-level military–civil fusion<sup>4</sup> (MCF) program that masks Beijing's strategic positioning in the guise of civilian, commercial activity—that of, say, a private electric bus company.

### State Financial Support

CRRC is a State-owned enterprise controlled by the Chinese State Council's State-Owned Assets Supervision and Administration Commission (SASAC).<sup>5</sup> CRRC's core and original business is the manufacture of rolling stock. It is the largest such manufacturer in the world. But through subsidiaries, investments, and partnerships, in China and abroad, CRRC's business extends more broadly, covering the entire land transportation ecosystem. CRRC's apparatus includes 46 wholly and majority-owned subsidiaries.<sup>6</sup> They reflect a presence across all of the rail industry's value chain, as well as emerging, adjacent domains: New materials, alternative energy sources, electric motors and transmissions, sensor networks, autonomous driving, semiconductors, energy storage. CRRC focuses in particular on “smart transportation” and data systems.

CRRC is one of the most heavily subsidized companies in China. Since 2015, CRRC has reported more than 6 billion RMB (over 850 million USD) in direct subsidies, with 1.37 billion RMB (or approximately 191 million USD) in 2018.<sup>7</sup> CRRC's 2019 subsidies likely exceeded that figure.<sup>8</sup>

<sup>3</sup>Planning for that industrial strategy was completed in January. It is expected to be released in March. [“China Standard 2035” Project Concluding Meeting and “National Standardization Development Strategy Research” Project]. State Administration for Market Regulation, January 14, 2020.) For additional discussion, see Emily de La Bruyere and Nathan Picarsic, “Game of Phones: 5G Is the Next U.S.–China Standards Battleground”, The Octavian Report, Summer 2019, <https://octavianreport.com/article/5g-us-china-standards-fight/>.

<sup>4</sup>Emily de La Bruyere and Nathan Picarsic, Military–Civil Fusion: China's Approach to R&D, Implications for Peacetime Competition, and Crafting a U.S. Strategy, 2019 NPS Acquisition Research Symposium, May 2019; Emily de La Bruyere and Nathan Picarsic, “Military–Civil Fusion: Crafting a Strategic Response”, CHIPS (DoN CIO Magazine), July–September 2019, <https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=12635>.

<sup>5</sup>The Chinese Government owns 53 percent of CRRC through the Chinese holding company China Railway and Rolling Stock Group Corporation. (CRRC Annual Report, 2018). As a CRRC representative put it in 2016, “CRRC's actual controller is a State-owned fund. CRRC is thus a State-owned entity.” ([Sun Pengcong]. [Nature of Property Rights, Government Support, and Financial Risks of M&A]. Inner Mongolia University, 2016.)

<sup>6</sup>Or, at least, its website declares that figure: CRRC's 2018 annual statement lists investments in 51 subsidiaries. And according to reports from its 2018 audit, in 2016 it declared 401 wholly owned and holding subsidiaries as well as 109 shareholding companies. [Audit Commission: CRRC and Other Super Companies Total Expenditure Subsidy of 647.3 Million], Audit Commission, June 20, 2018.

<sup>7</sup>[CRRC Corporation Annual Report], 2015 through 2018.

<sup>8</sup>As of June, CRRC had already reported 632.87 million RMB in direct subsidies. ([CRRC Corporation Limited Semi-annual Report 2019], 2019).

This financial backing is orders of magnitude higher than what CRRC discloses in its English language annual reports.<sup>9</sup>

Still, these figures likely underestimate the true degree of Government financial support fueling CRRC. They do not account for the beneficial tax cuts that fund much of CRRC's research and development (R&D)<sup>10</sup>—or, of course, any subsidies that CRRC chooses not to declare.<sup>11</sup> Nor do these figures account for the indirect support that CRRC receives: The State-owned enterprise benefits from an entire ecosystem of Government-backed R&D programs, innovation centers, national projects, and laboratories, many of which it oversees. And where CRRC has not vertically integrated, it further benefits from a domestic supply chain comprised of additional State-owned and State-backed vendors. The CCP also helps to set up CRRC's international contracts, marketing it as a One Belt One Road champion.<sup>12</sup>

Proportionately speaking, BYD receives even more State support than does CRRC. BYD has reported a total of 9.2 billion RMB (1.3 billion USD) in Government grants and subsidies since 2007. The company declared 2.3 billion RMB (approximately 328 USD million) in Government subsidies in 2018 alone. Those funds constituted more than half of BYD's total profit. In the third quarter of 2019, while Congress was debating the Transit Infrastructure Vehicle Security Act (TIVSA), BYD declared over RMB 1 billion more in direct Government subsidies.<sup>13</sup> Relative to profit, BYD is the single most subsidized Chinese player in its field.

As with CRRC, these figures likely constitute a lower-bound of the true magnitude of Government support. They omit, for example, consumer-side subsidies that reduce the price of electric vehicles in China: CITIC Securities estimates that BYD received an additional 37.3 billion RMB (5.3 billion USD) of such subsidies between 2016 and 2018.<sup>14</sup>

BYD is not a State-owned Enterprise. But it is guided by the Chinese Government. In fact, BYD's CCP connections are all the more threatening for its private status. Beijing knows that the U.S. and other international systems treat private companies as neutral actors. So, Beijing leverages those as masked vehicles for its offensive. In November 2018, the Ministry of Transportation invited BYD, as well as 19 other private companies,<sup>15</sup> “to discuss the role of private capital in building a Transportation Great Power.” The Minister promised “unwaveringly to encourage, support, and guide the private enterprises to become bigger, stronger, and better.” In return, he reminded them that they were to “contribute to the grand strategy and platform of a ‘Transportation Great Power’.”

“It is hoped that the majority of private entrepreneurs will better integrate into the tide of reform and opening up in the new era, actively participate in the construction of a Transportation Great Power, and work tirelessly to realize the Chinese dream of the great rejuvenation of the Chinese Nation.”<sup>16</sup>

CRRC and BYD's State backing is not unique. They are just two players in a much larger constellation. The National New Energy Vehicle (EV) subsidy program through which BYD received more than RMB 3.45 billion in 2018 also funded Foton Motor, Yanzhou Yaxing, BAIC Blue Valley, Ankai Automobile, Dongfeng Motor, Yutong Bus, Zhongtong Bus, etc. Tesla's largest Chinese competitor, Nio, benefits from the same demand-side EV subsidy as BYD.

<sup>9</sup> CRRC's English language annual reports suggest that it received approximately 243 million RMB (about 34 million USD) in “Government grants” in 2018 and 994 RMB (about 140 million USD) in 2017.

<sup>10</sup> In 2018, the State Administration of Taxation increased the tax deduction for R&D expenses from 50 percent to 75 percent, a deduction that “basically subsidizes 11 to 18 percent of actual R&D.” Vice President of CRRC Zhan Jingyan explained in March that, for CRRC, which invests about 10 billion (about 1.4 billion USD) annually into R&D, that amounts to “at least 1 billion RMB [about 140 million USD] of subsidies a year.” ([1 billion plus 600 million: After the tax and fee reduction, how much can CRRC save?]. *East Money Finance*, March 30, 2019.)

<sup>11</sup> CRRC has limited incentive publicly to report the full extent of Government financial support that can otherwise be obscured—and the Chinese State can easily funnel funds to companies that it owns.

<sup>12</sup> Premier Li Keqiang is called the “super salesman” of CRRC. ([Sun Peng Cong]. [Nature of Property Rights, Government Support, and Financial Risks of M&A]. Inner Mongolia University, 2016.)

<sup>13</sup> [BYD Annual Reports], 2009 through 2018; [BYD Third Quarterly Report], 2019.

<sup>14</sup> Glonway, “The Story of the BYD Government Subsidy”, *Sina Finance*, July 29, 2019.

<sup>15</sup> Huachuan Group, Land Bridge Group, Juneyao Airlines, SF Express, SJTI, Intech, Baidu, Didi, Ctrip, Deppon Logistics, Hecheng Group, Jinling Transportation, Chongqing Heniu, Fujian Air China, Guangxi New Harbor Engineering, Fujian Port Road, Beijing E-Hualu Information Technology, Kahangtianxia, and Shanghai Public Transport.

<sup>16</sup> [The Ministry of Transport invited 20 private enterprises such as SF, BYD, Baidu, Didi and others to encourage private capital to participate in transportation projects], China Communications News, November 22, 2018.

The CCP is pursuing a comprehensive program to dominate the international transportation supply chain, industry, and market. That program is part of Xi Jinping's "Transportation Great Power" strategy. The objective does not end at industrial development. This strategy is about asymmetric dependence, network control, and the international, coercive power to be reaped from those.

#### *Military Ties*

China's transportation agenda falls under the rubric of the national-level military-civil fusion strategy, a program that deftly inserts thinly veiled military tools into the fragmented, open global commercial ecosystem for coercive ends. "Military and civilian are different only in name," explain Chinese sources, "The military is for civilian use, and the civilian for military."<sup>17</sup> Transportation is key to this strategy. According to Chinese classifications, transportation falls squarely under the definition of a military industry.<sup>18</sup>

CRRC and BYD's ties to the People's Liberation Army (PLA) bear this point out. Both companies publicly espouse support for military-civil fusion, partner with military entities, and define their projects—especially in new energy automobiles, new materials, high-speed rail, and autonomous vehicles, and information systems—as part of the military-civil fusion program.

CRRC's annual report endorses the military-civil fusion strategy:

We will implement the military-civil fusion development strategy and expand the application of technology and products.

That is no empty claim. In May 2017, CRRC joined a series of State military and financial entities to spearhead a 113.9 RMB billion Government investment fund dedicated to military-civil fusion.<sup>19</sup> CRRC calls its High-Speed Train Technology Innovation Center a "military-civil fusion project."

In 2018, CRRC signed a "strategic cooperation agreement" with AVIC, a State-owned military enterprise, to launch an "MCF development program" dedicated to new materials, unmanned subways, and autonomous driving.<sup>20</sup> Meanwhile, BYD boasts a "strategic cooperation" agreement with the China Academy of Launch Vehicle Technology. The two seek jointly to develop to materials, guidance, sensors, fasteners, and autonomy, among other fields.<sup>21</sup>

CRRC and BYD also operate R&D centers in "military-civil fusion enterprise zones," industrial zones dedicated to incubation of, as well as information exchange among, MCF entities. BYD sits in the Beijing Daxing MCF Industrial Zone,<sup>22</sup> the Xi'an High-Tech Industrial Development,<sup>23</sup> and the Baotou Equipment Manufac-

<sup>17</sup>Ma Qing Feng, "Research on the Synergy Between Defense Economy and National Economy". Henan University, 2013. Ma wrote that text under the tutelage of Henan University's Sun Siquang, former senior scholar at the Chinese Academy of Social Sciences, consultant expert at the Small and Medium Enterprise Research Center of the Ministry of Industry and Information Technology (the Government entity charged with implementing MCF), and director of the Chinese Capital Research Society.

<sup>18</sup>In January 2018, the Ministry of Transport and the National Defense Science and Industry Bureau signed a cooperation agreement to promote, together, military-civil fusion. A 2018 article from the Army Military Transportation Institute is sufficiently on the nose: "Under the conditions of informationization, the military increasingly depends on national transportation and communications resources. To strengthen the construction of strategic projection capabilities, it is necessary to use national strategic transportation resources to establish a military-civil fusion strategic projection system. Recently, China's transportation infrastructure has achieved unprecedented development, so that civil transportation infrastructure and large-scale transportation vehicles can not only help economic construction but also directly support national defense and military needs to improve our military's strategic projection capabilities." ([Zhang Jian], [Meng Jun], [Yang Xikai], [Research on the Military-civilian Integrated Development of National Defense and Transportation in the New Period], 2018.)

<sup>19</sup>[China CRRC: Capital to set up a scale of 113.9 billion funds, investing in military and civilian integration and other industries]. [China Fund News], July 3, 2017

<sup>20</sup>[AVIC and China's CRRC affiliated enterprises signed a military-civilian integration development project cooperation agreement], Sohu News, May 25, 2018.

<sup>21</sup>[BYD will conduct strategic cooperation with China Academy of Launch Vehicle Technology], Xinhua, April 7, 2018.

<sup>22</sup>Approved by the Ministry of Industry and Information Technology (MIIT) in 2012, the Beijing Daxing Industrial Base focuses on aerospace technology, the weapons industry, new materials, and new energy. It hosts, among others, NORINCO, AVIC, and the China Rocket Corporation.

<sup>23</sup>That zone takes, as its "main direction," "absorbing high-quality resources from the whole society to participate in national defense construction, guiding civilian technology to expand into the military field, and promoting network information." (Xi'an High Tech Industrial Development Zone, xdz.gov.cn)

turing Industrial Park.<sup>24</sup> The Harbin Economic and Technological Development Zone that hosts a CRRC R&D center is also home to Harbin North Defense Equipment Co., Ltd, AVIC's Dong'an Engine Group, Chinalco's Northeast Light Alloy Co., and "other important military enterprises." Those zones, and others like them, support their members financially. They also create channels for "research integration;" mechanisms for sharing technological and data resources.<sup>25</sup>

CRRC and BYD also partner with other MCF players that the United States has already labeled as predatory actors or national security threats. Both companies signed "strategic cooperation agreements" with Huawei in March 2019. The BYD-Huawei relationship focuses on automotive intelligent networking, intelligent driving, cloud computing, and smart parks;<sup>26</sup> the CRRC Huawei partnership on connecting the former's physical, rail infrastructure to the latter's information technology.<sup>27</sup>

### A Transportation Great Power and Network Hegemony

How does this all actually add up? The Huawei relationships begin to frame the picture. Beijing is not undercutting U.S. companies simply to subvert American manufacturing. (Though they do.)

Beijing is not deploying information-collecting systems simply to spy on critical U.S. hubs. (Though, again, this first-order risk is real.) Beijing targets the transportation industry in order to can capture foundational, physical and virtual, infrastructures. It intends to set global rules.

Beijing establishes its footholds in physical infrastructure. It extends its reach through information infrastructure. Made in China 2025 outlines that first phase: Monopoly over global industry's critical physical components. China Standards 2035, to be officially launched this month, defines the next step: Beijing's plan for dominance over global rules.

According to official State planning, China intends to establish a "global smart grid" connecting new energy sources and a "global transportation system" connecting smart vehicles. China intends to proliferate "sensor networks" and a "global logistics platform." It intends to link all of these on a "ubiquitous," "backbone" "Internet of Things (IoT)"—or "Internet of Everything;"<sup>28</sup> the future foundation for military, commercial, social, political, information narrative domains. In sum, it intends to build the tracks, pipes, channels along which everything in the information era operates; having built those, to collect and to define their information.

If China realizes this vision, it will acquire immediate information access—with obvious first order security risks. In the longer term, Beijing's network will also allow it to shape information; therefore both to coerce and to define the global environment. This would amount to unprecedented, cross-domain, new-type power projection.

Transportation systems offer an entry point.

On September 23, 2019—as this body was debating the TIVSA—the Central Committee of the Chinese Communist Party and the State Council issued the "Transportation Great Power Outline." "By 2035, a transportation powerhouse will be basically established." Having cemented dominant international positions in transportation equipment, hubs, systems, standards Beijing will deploy a global a system of "three-dimensional interconnection," linking "railways, highways, waterways, civil aviation, pipelines, postal services, and other infrastructures."<sup>29</sup>

The Chinese transportation network will be the foundation for global movement. It will also offer the Chinese Communist Party complete information on that movement. "Integrated with big data, Internet, AI, blockchain, super-computing," it is to feed into a Government-run "comprehensive transportation big data center."<sup>30</sup> It

<sup>24</sup>The Baotou Zone's members include China Weapon First Machinery Group and NORINCO's engineering machinery group.

<sup>25</sup>The Xi'an Zone—which connects almost 1,000 universities and military units to its companies—includes a "Xi'an Science and Technology market" for "transaction, sharing, and communication" to provide "technical exchange and equipment sharing for military-civil enterprises." It organizes "matchmaking meetings, technical seminars, investment promotion associations, and MCF markets." (Xi'an High Tech Industrial Development Zone, [xdz.gov.cn](http://xdz.gov.cn))

<sup>26</sup>[BYD and Huawei will hold hands again: cooperation will be carried out in the areas of car networking and smart driving], March 26, 2019.

<sup>27</sup>[The company cooperates with Huawei to build an industrial internet platform]. CRRC, April 2, 2019.

<sup>28</sup>"National Medium- and Long-Term Program for Science and Technology Development (2006–2020)", Ministry of Science and Technology, Beijing: 2006.

<sup>29</sup>Outline of Building a Powerful Country for Transportation, Central Committee of the Communist Party and the State Council, September 2019.

<sup>30</sup>In December, 3 months after the State Council published the Transportation Great Power Strategy, the Ministry of Transportation issued a supporting plan for "Promoting the Develop-

will connect to other domains—“energy networks, information networks”—as well as military systems, including China’s “Beidou satellite navigation system.”<sup>31</sup>

The system is to permit “global big data analysis.” It is to support “national strategies,” including both the Transport Great Power Strategy and One Belt One Road. It is to be fully established by 2025. “Notice of the Ministry of Transport on issuing the ‘Outline Action for Promoting the Development of Comprehensive Transportation Big Data 2020–2025’”, Ministry of Transport, December 12, 2019.)

This network will extend internationally through the unwitting cooperation of foreign actors. China’s Transportation Great Power Strategy explains that the network will spread via the corridors of the Silk Road Economic Belt; fueled by “international investment” (albeit only from those entities that pass the Corporate Social Credit System’s screening) and based on partnerships among Chinese companies and foreign States, societies, and enterprises<sup>32</sup>—partnerships like, of course, those between BYD and CRRC and the U.S. system.

In October, BYD General Manager Li Hui declared his company a champion of “Xi Jinping’s Transportation Great Power” strategy.<sup>33</sup> CRRC’s President Sun Yongcai spoke even earlier and more explicitly of CRRC’s participation: “The National Congress of the Communist Party of China has proposed to build a ‘technological power, quality power, aerospace power, network power, and transportation power,’” he said in 2018. “Facing the trend of the times and the golden opportunity, CRRC will shoulder the responsibility of carrying out national strategy.”<sup>34</sup>

Beijing intends to complete its transportation vision by 2035. But the foundation is in place, globally, today. The Transportation Great Power strategy describes a multidimensional logistics network. Through foreign investments, commercial proxies, and cooption of multilateral organizations, China has already established that network. It is called the National Transportation Logistics Platform in China; LOGINK abroad. No one is talking about it. It connects the global ports, rail, air, post systems in which China invests to a domestic data hub. Beijing has secured the support of ASEAN’s NEAL-NET and Europe’s IPCSA so that they proliferate China’s information system, so that Japan and South Korea advocate a Chinese coercive tool as a global standard. Ostensibly private Chinese companies extend the net more widely and more subversively. Alibaba’s Cainiao Logistics maintains a strategic cooperation agreement with LOGINK. Relationships with Alibaba proliferate the Chinese State data system.

This constitutes an entirely new type of power projection. Interconnected global networks and platforms risk granting Beijing unprecedented coercive might. China’s web of smart cities, telecommunications, surveillance, logistics platforms, land and sea transportation, e-commerce, FinTech empower the CCP to shape, deny, and coerce—informationally, economically, and kinetically. Recent jamming at the port of Shanghai points to potential first order, operational threats. China’s corporate social credit system does the same in the economic domain. But proliferated through ostensibly commercial rather than explicitly military tools, this subversive web is escaping our attention. Worse yet we are fueling it. We should not be granting Federal funding to China’s State-supported champions.

---

ment of Comprehensive Transportation Big Data (2020–2025). That plan orders all entities under the central Government to cooperate in the construction of a “multidimensional,” “controllable,” “integrated,” “comprehensive transportation big data system.”

<sup>31</sup>[Outline of Building a Powerful Country for Transportation], Central Committee of the Communist Party and the State Council, September 2019.

<sup>32</sup>[Outline of Building a Powerful Country for Transportation], Central Committee of the Communist Party and the State Council, September 2019.

<sup>33</sup>He also advertised the links between BYD and Huawei: “Our communication and signal systems use ITE-U in cooperation with Huawei.” ([2019 Global Future Travel Conference; Li Hui, General Manager of BYD Rail Business]. *auto.gasgoo.com*, October 30, 2019.)

<sup>34</sup>[Sun Yongcai: Contributing CRRC Solutions and CRRC Wisdom to the Construction of a Powerful Transportation Country], *Sina Auto*, January 20, 2018.

**PREPARED STATEMENT OF FRANK J. CILLUFFO**

DIRECTOR, MCCRARY INSTITUTE FOR CYBER AND CRITICAL INFRASTRUCTURE SECURITY, AND DIRECTOR, CENTER FOR CYBER AND HOMELAND SECURITY, AUBURN UNIVERSITY

MARCH 5, 2020

**Introduction**

Chairman Crapo, Ranking Member Brown, and distinguished Committee Members—notably including Senators Shelby and Jones from my Institute’s home State of Alabama—thank you for the opportunity to testify before you today.

The threats to public transportation posed by State-owned and State-supported enterprises is a matter of national significance, as the issue bears on U.S. national and economic security, which are inextricably intertwined. Your leadership in this area is important and commendable, not least because the concerns that are at play in regards to public transportation apply also to other critical U.S. infrastructure sectors and national critical functions.<sup>1</sup>

Fortunately, the subject under study today has been the focus of considerable attention on the part of lawmakers in recent months. Much credit is, of course, due to this Committee’s Chairman and Ranking Member, together with Senators Cornyn and Baldwin (also testifying today), for leading the charge on legislation in this area.<sup>2</sup>

By way of further example, last May, your colleagues on the House of Representatives’ Committee on Transportation and Infrastructure also convened a hearing similar to this one, at which I also had the privilege of testifying.<sup>3</sup> My statement before you today builds on my statement of last year, and I will take a parallel approach: first, I will set out the threat and place it in context, showing why it matters; and second, I will offer selected policy recommendations that speak to priority issues requiring timely action.

**The Threat Climate and Its Implications**

This hearing speaks specifically to the threat posed to public transportation by State-owned and State-supported enterprises. On this question, let me speak plainly: the chief threat comes from China and certainly includes the sale and provision of railway cars to U.S. transit systems—but the threat also extends far beyond, to much more than the transportation sector alone.

The crux of the matter is that State-owned and State-supported enterprises are able to outbid others when competing for contracts. In the case of China, a non-market economy, this is part of a broader strategy to undermine America’s economic might; and the challenge is not just economic. This is so because U.S. national and economic security are inextricably interwoven. Each depends upon the other.

From a cyberstandpoint, a State-owned enterprise (Chinese or otherwise) foothold into the supply chain of public transportation, a critical U.S. infrastructure sector, could open the door to a wealth of intelligence that could be weaponized against us. While there are a multitude of ways to engage in espionage, the line between it (computer network exploitation) and computer network attack is thin and turns largely on intent. Put differently, if you can exploit, you can also attack, if the will exists to do so.

This begs the question, why open this door to espionage as potential gateway for attack, if it is not necessary to do so?<sup>4</sup> Keep in mind that espionage in this context could allow an adversary to map critical U.S. infrastructure prior to attack and otherwise engage in intelligence preparation of the battlefield (as the military would say). While, in general, security is not the only factor to be considered in decision-making in this context public safety should be the larger concern, especially given the potential for hybrid (not just cyber but physical) consequences.

<sup>1</sup> The National Risk Management Center (NRMC) has identified and created a list of National Critical Functions that addresses cross-sector and systemwide risks. NRMC is nested within the Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA). For details, see <https://www.cisa.gov/national-critical-functions>.

<sup>2</sup> S. 846, Transit Infrastructure Vehicle Security Act, <https://www.congress.gov/bill/116th-congress/senate-bill/846/cosponsors?searchResultViewType=expanded&KWICView=false>.

<sup>3</sup> “The Impacts of State-Owned Enterprises on Public Transit and Freight Rail Sectors”, (May 16, 2019), <http://cchs.auburn.edu/~files/the-impacts-of-state-owned-enterprises-on-public-transit-and-freight-rail-sectors.pdf>. This statement should be read in tandem with the present written testimony, since I have not repeated all of the details here.

<sup>4</sup> To be clear on the issue of necessity in the context of railcars in particular, there do exist alternatives for U.S. transit systems to pursue instead of purchasing from Chinese State-owned or State-supported enterprises. See below for additional details.

In case the above is a bit too abstract to appreciate fully, let me explain more concretely the cybersecurity risks associated with railcars produced by State-owned enterprises: the potential for continuous and purposeful (adversary) access to our railcar/transit systems may arise through equipment communications links; hardware or software may be compromised; and the likelihood of direct access is real.<sup>5</sup>

Consider just some of the consequences that could follow from these risks: the adversary could shut down trains and disrupt transit operations; knock-on effects could hit other critical U.S. infrastructure sectors; and major U.S. cities that depend strongly on rapid transit systems could experience significant economic effects, particularly if an incident were to disrupt systems for a lengthy period.

It is important to note that State-owned and State-supported enterprises may not even be witting accomplices in any of this. While certain countries (such as China and Russia) have laws that require State-owned enterprises to furnish assistance upon request,<sup>6</sup> such companies may also be inadvertent conduits for furthering the goals and ambitions of their (authoritarian) State of origin.

Despite this array of serious security implications, America has yet to inoculate itself against them. I will not repeat here all of the case-specific evidence offered in my 2019 testimony.

Suffice it to say, for the sake of illustration, that China Railway Rolling Stock Corporation (CRRC) is building new railcars for major American cities such as Boston, Chicago, Los Angeles, and Philadelphia. This gives rise to a plethora of vulnerabilities as described.

The temptation to procure from CRRC is understandable from the perspective of cost alone; State subsidies tilt the playing field heavily in China's favor.<sup>7</sup> But there is so much more than price at play here: China is not just seeking to win in U.S. markets<sup>8</sup>; it has developed and is executing a much larger strategy (Made in China 2025<sup>9</sup>) designed to further the country's economic, military, and political goals.

A forthcoming analysis of 464 documented cases of China's espionage worldwide concludes that "collection efforts coordinate closely to the priority technologies identified in Government strategic planning documents," including Made in China 2025, and Space Science and Technology in China: A Road Map to 2050. Chinese "private companies" and State-owned enterprises each engage in or support espionage in just over 21 percent of the cases studied; and together constitute slightly more than 43 percent of the case total. Targets include "U.S. military and space technologies" and "commercial interests."<sup>10</sup>

<sup>5</sup>Via onsite employee (State-owned enterprise employee or contractor sited at U.S. transit agency) with access to networks/operations.

<sup>6</sup>In the case of China, at least three instruments are at play: the National Intelligence Law of 2017, the associated Implementing Regulations, and Communist Party requirements enshrined in law and iterated publicly in 2014, 2015, and 2017. For details, see Nick Eftimiades, "On the Question of Chinese Espionage" (forthcoming), *Brown University Journal*.

<sup>7</sup>For a long-form examination of a case of Chinese underbidding giving rise to quality control concerns and costs that ultimately "ballooned" see: Charles Piller, "Troubled Welds on the Bay Bridge: How a Chinese Builder's Flaws Left Structural Doubts and Cost Taxpayers", *The Sacramento Bee* (June 7, 2014), <https://www.sacbee.com/news/investigations/bay-bridge/article2600743.html>.

<sup>8</sup>Even in relation to the narrow issue of trying to win in U.S. markets however CRRC has been engaged in a "misinformation campaign"—as noted in a compelling letter of warning to Secretary of Transportation Elaine Chao (dated February 13, 2020) from Senators Cornyn and Baldwin. In the Senators' words: "The CRRC has used the argument that no U.S. companies manufacture transit railcars and if not for CRRC we would have no railcars in America. This does not take into account that the U.S. has a thriving and robust transit rail manufacturing sector . . . which is comprised of numerous enterprises from market economy allies of the U.S. Most importantly, unlike CRRC, these companies use U.S. supply chains, use U.S. produced components, and are compliant under 'Buy America' provisions." <https://www.documentcloud.org/documents/6781588-Cornyn-Baldwin-TIVSA-Implementation.html>

<sup>9</sup>"The Made in China 2025 Initiative: Economic Implications for the United States", Congressional Research Service—*In Focus* (updated April 12, 2019), <https://fas.org/sgp/crs/row/IF10964.pdf>. In a 2018 speech to China's National Academy of Sciences and Engineering, President Xi Jinping asserted: "If China is to flourish and rejuvenate, it must vigorously develop science and technology and strive to become the world's major scientific center and innovative highland. Self-reliance is the basis for the struggle of the Chinese Nation to stand on its own footing in the world." Cited in Simon Sharwood, "Chinese President Xi Seeks Innovation Independence", *The Register* (June 1, 2018), <https://www.theregister.co.uk/2018/06/01/xi-xinping-science-technology-policy-speech/>.

<sup>10</sup>Eftimiades, "On the Question of Chinese Espionage". Note also: Department of Justice Office of Public Affairs, "Newly Unsealed Federal Indictment Charges Software Engineer With Taking Stolen Trade Secrets to China" (July 11, 2019), <https://www.justice.gov/opa/pr/newly-unsealed-federal-indictment-charges-software-engineer-taking-stolen-trade-secrets-china> [A soft-

Continued

Put bluntly, China's strategy is powered by theft of U.S. intellectual property; and we ignore or underplay that broader context at our peril. In the words of the new U.S. National Counterintelligence Strategy released last month by the National Counterintelligence and Security Center: "A more powerful and emboldened China is increasingly asserting itself by stealing our technology and intellectual property in an effort to erode United States economic and military superiority."<sup>11</sup>

The scale and scope of the challenge is daunting. According to FBI Director Christopher Wray, "The FBI has about a thousand investigations involving China's attempted theft of U.S.-based technology in all 56 of our field offices and spanning just about every industry and sector. U.S. companies and U.S. universities are both targets—all over the country, from Alabama to Iowa."<sup>12</sup> The situation is all the more concerning when set against China's plans to double its current spending on research (\$400 million) to \$800 million. It is expected that these monies will be directed primarily to the country's Thousand Talents Program (for recruitment) and the buy-out of bankrupt companies.<sup>13</sup>

In addition, economic and political power are (of course) tightly connected. As press reports note, "China's influence playbook centers around economic leverage stemming from its growing wealth." The FBI's Foreign Influence Task Force notably includes a unit dedicated to "countering China's political influence in the United States."<sup>14</sup>

Against this backdrop, the new U.S. National Counterintelligence Strategy articulates five Strategic Objectives that require a whole-of-society approach, including the following that are of particular relevance to today's hearing: Protect the Nation's Critical Infrastructure; Reduce Threats to Key U.S. Supply Chains; and Counter the Exploitation of the U.S. Economy.

Returning specifically to transportation, against this broader background, rail is not the only concern: by way of further example, a Chinese manufacturer (DJI) has captured the U.S. market for unmanned aircraft systems (UAS).<sup>15</sup> The end-user of these systems may be a range of critical U.S. infrastructure sectors, and sensitive data may be exposed.<sup>16</sup>

The transportation sector as a whole also intersects with and supports other critical U.S. sectors and national functions. Notably, U.S. national defense is to an extent dependent upon the integrity of the transportation sector. If compromised, the ability of U.S. forces to deploy, project power, and achieve their goals and objectives (collectively known as Mission Assurance), may be placed into jeopardy.<sup>17</sup> Consider the potential for cyber/physical convergence, with concomitant consequences on the battlefield.

Widening the aperture further, foreign State-owned enterprises and the advanced technologies that they offer, at relatively low cost and often with concessionary financing, pose a dilemma for other critical infrastructure sectors as well. Case in point: 5G telecommunications technology from Chinese companies Huawei and ZTE.

---

ware engineer at a suburban Chicago locomotive manufacturer stole proprietary information from the company and took it to China].

<sup>11</sup> National Counterintelligence Strategy of the United States of America 2020–2022, <https://www.dni.gov/files/NCSC/documents/features/20200205-National-CI-Strategy-2020-2022.pdf>.

<sup>12</sup> Catalin Cimpanu, "FBI Is Investigating More Than 1,000 Cases of Chinese Theft of U.S. Technology", *ZDNet* (February 9, 2020), <https://www.zdnet.com/article/fbi-is-investigating-more-than-1000-cases-of-chinese-theft-of-us-technology/>. Note also, the FBI "made 19 arrests this fiscal year alone on charges of Chinese economic espionage. In comparison, the FBI made 24 arrests all last fiscal year, and only 15, five years earlier, in 2014." *Ibid.* See also: Jackson Cote, "China's Economic Espionage and Theft Is a Real, [sic] U.S. Attorney Andrew Lelling says after arrest of Harvard professor for undisclosed ties to China", *MassLive.com* (January 28, 2020), <https://www.masslive.com/boston/2020/01/chinese-economic-espionage-and-theft-is-a-real-us-attorney-andrew-elling-says-after-arrest-of-harvard-professor-for-undisclosed-ties-to-china.html>

<sup>13</sup> Telephone interview with Nick Eftimiades on February 18, 2020.

<sup>14</sup> Bethany Allen-Ebrahimian, "Exclusive: How the FBI Combats China's Political Meddling", *Axios* (February 12, 2020), <https://www.axios.com/fbi-china-us-political-influence-0e70d07c-2d60-47cd-a5c3-6c72b2064941.html?stream=top>.

<sup>15</sup> Consider also: in their recent letter to Transportation Secretary Chao, Senators Cornyn and Baldwin underscore and detail the threat posed to the United States by Chinese buses (in addition to railcars). <https://www.documentcloud.org/documents/6781588-Cornyn-Baldwin-TIVSA-Implementation.html>

<sup>16</sup> See my 2019 testimony for allegations to this effect raised by U.S. officials in 2017. An additional concern, more generally, is the potential for data manipulation. In the financial services sector, for instance, transactions take place in milliseconds. The ability to slow the transmission of signals could allow a malicious actor to attain control or dominance of the market. Eftimiades interview (February 18, 2020).

<sup>17</sup> Auburn University Center for Cyber and Homeland Security, "Strengthening Defense Mission Assurance Against Emerging Threats" (May 2019), <http://cchs.auburn.edu/files/mission-assurance-policy-forum-summary.pdf>.



5G is the bedrock for next-generation networks worldwide. The strategic significance of 5G is reflected in the Prague Proposals, recognized by more than 30 countries worldwide.<sup>18</sup> Who builds and contributes to these networks matters deeply, and each country's decision on the matter will affect not only their telecommunications sector but also every other sector and function that depends on telecommunications (such as transportation, including autonomous vehicles).

Huawei and ZTE are competing aggressively to serve as suppliers worldwide; but America is rightfully taking a hard line at home and urging allies to do the same, based on evidence of these two companies' complicity with the Chinese Government. Just last month, the U.S. Department of Justice revealed new charges against Huawei, citing racketeering and conspiracy to steal trade secrets.<sup>19</sup>

Other products and technologies supplied by Chinese companies that have raised security concerns in the United States include video surveillance equipment manufactured by Hangzhou Hikvision Digital Technology and used in U.S. schools and other sensitive (military/diplomatic) sites. At inception, Hikvision was a Chinese Government research institute. State-owned enterprises retain a 40-plus percent stake in the company.

Many other smaller but still important opportunities exist for foreign State-owned enterprises to make inroads into U.S. critical infrastructure sectors either directly or indirectly. Flush with State support, these foreign enterprises can buy up U.S. assets/entities that are on the verge of bankruptcy or in need of start-up funding. Such acquisitions may relate only to a component, such as switches; but switches are key to the safe operation of passenger and freight rail.

In the context of rail transit systems, switches and precision timing go hand-in-hand. The wider trio of issues—positioning, navigation, and timing (PNT)—also merits a quick sidebar: China is investing heavily to safeguard its own PNT functions and undermine those of others (including through antisatellite capabilities that could blind and bind the U.S. military, which relies heavily on space-based assets for transit and targeting requirements and other needs).<sup>20</sup>

Whether in relation to the transportation sector or beyond, supply chain and concomitant counterintelligence and national security concerns are certainly not limited to Chinese-origin goods and services. Russian antivirus software produced by Kaspersky Lab, for example, poses similar concerns and for this reason is subject to a ban on use by U.S. Federal agencies.

A final word on threat: the Internet of Things raises further the salience of the concerns expressed here as it continues to expand the potential surface of attack; think sensors, smart cities, and smart cars. While it may not be possible to eliminate all vectors of attack, it is imperative that we seek to limit them and at the same time, cultivate resilience—the ability to minimize the impact of, and bounce back from, an incident.

### Selected Policy Recommendations

Turning to counterthreat measures, I would be remiss if I did not begin by giving credit where it is due. A solid step in the right direction is S. 846, the Transit Infrastructure Vehicle Security Act. This legislation, cosponsored by Chairman Crapo and Ranking Member Brown (plus others including Senators Shelby and Jones), represents precisely the sort of precautionary action needed.<sup>21</sup>

With its incorporation into law as part of the National Defense Authorization Act (NDAA) for Fiscal Year 2020, new public transit system railcars will be subject to cybersecurity certification; a specific category of countries of concern will be barred from participating in rolling stock procurement bids solicited by public transit sys-

<sup>18</sup>Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals", (March 5, 2019), <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>.

<sup>19</sup>"Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy To Steal Trade Secrets", (February 13, 2020), <https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering>.

<sup>20</sup>The new Executive Order on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing Services issued on February 12, 2020, is a welcome development. <https://www.whitehouse.gov/presidential-actions/executive-order-strengthening-national-resilience-responsible-use-positioning-navigation-timing-services/>

<sup>21</sup>S. 846 is the basis of language that was ultimately enacted into law in Section 7613 of the National Defense Authorization Act for Fiscal Year 2020 (P.L. 116-92).

tems; and the “next-generation” buildout of the National Capital’s rail transit system (Metrorail’s 8,000-series cars) will be insulated from penetration by CRRC.<sup>22</sup>

The provision (NDAA Section 7613) that speaks to cybersecurity certification underscores the importance of “third-party testing and analysis” in addition to “voluntary standards and best practices” developed under the aegis of the National Institute of Standards and Technology (NIST) and the Secretary of Homeland Security. This is a prudent and laudable approach. Certifications, underpinned by common standards and third-party testing, has proven successful in moving markets in other industries. In fact, I would go a step further and suggest that the general principles of the cited provision (Section 7613) should apply also to other critical infrastructure sectors.

In charting a course forward, the challenge is to maintain and enhance U.S. national security while limiting collateral damage to other U.S. interests. Put starkly, we must figure out a way to preserve and advance our security without undermining unduly the U.S. economy. While this need not be an either/or proposition, the way forward will require sustained leadership and determination on the part of both Government and industry, coupled with a willingness and ability to prioritize. More fundamentally, it may require us to look deeper at how to better leverage market forces to incentivize security. This may mean creating a greater demand for security from consumers in the products and services they buy. It may also mean incentivizing suppliers to prioritize security as a differentiator in the products they produce. Action will entail costs; but inaction will ultimately be far costlier.

In practice, therefore, we should begin with the Lifeline Sectors, which are the most critical of the critical. These include the defense industrial base, energy (electricity, oil, natural gas), financial services, transportation, telecommunications, and water. Together with the list of National Critical Functions identified by the National Risk Management Center, is a good place to start in terms of prioritizing our efforts to elevate and monitor security concerns, test our response and mitigation measures, and continually refine these regimes. All risk management proceeds in cycles, and national risk management is no exception. Risk identification, assessment, and management must be continuous, adaptive, and forward looking. A reactive or regulatory “check-the-box” approach simply will not do.

Part of this exercise must involve scrutinizing supply chains. While helpful steps have already been taken—such as Executive Order 13806 on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States<sup>23</sup>; and the Information and Communications Technology Supply Chain Risk Management Task Force launched by the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (CISA)—efforts must be widened and deepened.<sup>24</sup>

A “system of systems” approach is also needed on the technology side in order to properly integrate advancements into the broader ecosystem. To date, we have fallen short on this count. As remedy, an R&D effort is needed—in the form of a nationwide network of technology testbeds that simulate a realistic pansectoral environment. Taken in aggregate, such a platform would identify and explore the various national and economic security implications of new and critical technologies before they are in widespread use.

A strategic approach is equally needed in terms of integrating cyberfactors into our thinking and practices more generally, from the get-go, rather than retrofitting

<sup>22</sup>The Washington Metropolitan Transit Authority is poised to contract for its “next-generation” railcars; the deal could be worth over \$1 billion. Justin George, “Metro’s Next-Generation Rail Cars Will Not Be Made in China”, *Washington Post* (January 25, 2020), <https://www.washingtonpost.com/local/trafficandcommuting/metros-next-generation-rail-cars-will-not-be-made-in-china/2020/01/25/1d848c7e-3e06-11ea-baca-eb7ace0a3455-story.html>. For a helpful (plain-language) elaboration of some of the key implications of the relevant NDAA provision, see: Bethany Allen-Ebrahimian, “Senators Warn of Threats Posed by Chinese Rail Companies”, *Axios* (February 20, 2020), <https://www.axios.com/china-rail-car-threat-senators-transportation-beb72eaf-9c25-4dc0-a88a-f42d2a37d793.html>.

<sup>23</sup>July 21, 2017, <https://www.federalregister.gov/documents/2017/07/26/2017-15860/assessing-and-strengthening-the-manufacturing-and-defense-industrial-base-and-supply-chain>.

<sup>24</sup>Robert Kolasky, Director, National Risk Management Center (CISA, DHS): Statement for the Record for a Hearing on “Securing U.S. Surface Transportation From Cyber Attacks”, before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation (February 26, 2019), <https://www.congress.gov/116/meeting/house/108931/witnesses/HHRG-116-HM07-Wstate-KolaskyB-20190226.pdf> at p. 5. See also, DHS CISA et al., Internet of Things Security Acquisition Guidance—Information Technology Sector (February 2020), <https://www.cisa.gov/sites/default/files/publications/20-0204-cisa-sed-internet-of-things-acquisition-guidance-final-508-0.pdf>.

cyberfixes later on when damage is already done. By way of example, risk assessments and risk management strategies should not be treated as a separate vertical; instead, they should be integrated from inception. Along similar lines, a domestic version of The Prague Proposals<sup>25</sup> could prove useful for safeguarding U.S. Lifeline Sectors and National Critical Functions in relation to the rollout and widespread implementation of 5G technology. Ultimately, the United States must continuously identify the industries and technologies critical to national and economic security and take steps to reduce vulnerability at both a macroeconomic and microeconomic level.

In furtherance of much of the above (and to inform cyberpolicy and programs more generally), it would be helpful to have in place a dedicated and official entity that is tasked with collecting and providing data (statistics) on cybersecurity and the broader cyberecosystem. Both the Government and the private sector lack reliable, comprehensive, and empirical metrics on which to base public policy and risk management practices, respectively. We must seek to apply the same level of rigor, clarity, and statistical analysis to cybersecurity that we have given to public health, the economy, and criminal justice.

In addition, resources—both human and capital—are needed. To this end, building the Nation's cyberworkforce should be a national imperative and addressed urgently, as there is a disturbing deficit of knowledge and bandwidth in our public institutions and in our companies in relation to countering and thwarting cyberthreats posed by State actors to U.S. critical infrastructure.

Regarding the machinery of Government: in order to properly safeguard U.S. national and economic security in this context, the arms and legs of the U.S. Government will have to recalibrate their efforts and synchronize them ever more intensely to better support top-priority critical infrastructure and Nation critical functions. For example, the FBI is already working to lash up and grow its Cyber and Counterintelligence Divisions, in order to counter advanced and persistent adversary activity. This is a solid start, but must be continued, enhanced, and expanded over time. Another important partner in the mission is the National Security Agency and in particular its Cybersecurity Directorate. That entity's role in fusing foreign intelligence and cyberdefense will be instrumental to Department of Defense Mission Assurance (among other things).

Finally, I would like to add that the U.S. Cyberspace Solarium Commission, of which I am a member, took on many the above-discussed issues throughout the course of our work. Our forthcoming report, due out on March 11th of this year, lays a clear path forward to increase the effectiveness of U.S. Government collaboration, resilience of critical infrastructure, security of the cyberecosystem, and public-private partnership.<sup>26</sup> I look forward to continuing the conversation, and to working further with you and your colleagues in the weeks ahead, on these matters of national importance.

## Conclusion

Thank you for the opportunity to testify before you today.<sup>27</sup> I look forward to trying to answer any questions that you may have.

<sup>25</sup> These principles regarding the "cybersecurity of communication networks in a globally digitized world" were generated at the 5G Security Conference (2019) in which 32 countries participated. *Supra*.

<sup>26</sup> The Commission worked across industry, academia, the Congress, and the executive branch to arrive at workable solutions to strengthen the security posture of the United States in cyberspace. Our forthcoming report organizes nearly 80 recommendations across six pillars.

<sup>27</sup> Thank you also to my Deputy Director, Sharon Cardash (with Auburn's Center for Cyber and Homeland Security), for her skillful assistance in preparing this testimony.

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON  
FROM E. MICHAEL O'MALLEY**

**Q.1.** What other industries should Congress consider as potential vehicles for Chinese espionage? Are there any Chinese firms that you believe are flying under the radar in terms of dominating strategically important industries?

**A.1.** The railway supply industry is one of ten sectors that the Chinese Communist Party (CCP) has identified publicly in its Made in China 2025 initiative, and there is every reason to believe that China could use any of these sectors for espionage or other illicit activities. Our experience suggests that they are willing to go to great lengths to dominate these sectors and leverage that dominance to accomplish political and strategic aims.

While CRRC's penetration of the U.S. passenger railcar market has garnered the most attention to date, there are other rail-sector Chinese SOEs in other segments of the industry that would present equally concerning threats if they were to gain a foothold in the North American market. These companies include China Railway Signal & Communication (CRSC) and China Railway Engineering Corporation (CREC), both of which have been key players in China's rail projects around the globe.

**Q.2.** Given that China appears to blend the its militarily and civilian sectors in the service of a common political objective set by the Chinese Communist Party (CCP), would the United States be unreasonable to view powerful Chinese commercial firms as extensions and enablers of the Chinese military, and as instruments of the CCP?

**A.2.** The ties between Chinese SOEs like CRRC and the Chinese Government are well documented. CRRC's own bylaws explicitly state that the company must consult with the CCP on activities affecting the company's operations.<sup>1</sup> The company's board of directors also include many high ranking CCP officials, making it readily apparent that the mission of companies like CRRC are tied closely to that of the Government leadership. Thus, we should view the national security and economic risks associated with Chinese SOEs in the rail manufacturing sector as part of a single, integrated threat to U.S. economic and national security.

**Q.3.** It is also apparent that China is attempting to establish global information and standard-setting dominance by infiltrating little known standard-setting bodies to gain advantages. How could the U.S. dramatically raise China's cost of executing its current strategy?

**A.3.** Our members are actively working on a whole host of technologies, including IoT enabled solutions, that can deliver enhanced safety, security, and efficiency to the rail industry. It is critically important that we not allow Chinese SOEs to dictate the standards for those technologies given that critical shipments of military goods, hazardous materials, and people rely on them every day.

RSI continues to seek dedicated investment in infrastructure, balanced economic regulation and the promotion of domestic manu-

<sup>1</sup>"CRRC Corporation Limited Articles of Association", CRRC Corporation Limited, at 70; <http://www.crrcgc.cc/Portals/73/Uploads/Files/2018/6-4/636637164457871915.pdf>.

facturing to drive American innovation. We strongly encourage Congress to pass a surface transportation bill with dedicated and predictable funding for transit and intercity passenger rail to help increase domestic manufacturing of rolling stock and its associated technologies. Additionally, enacting regulatory reforms that ensure safety and encourage investments in innovative technologies would be another important step forward to mitigate China's attempt at standard setting dominance in this industry.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON  
FROM SCOTT N. PAUL**

**Q.1.** What other industries should Congress consider as potential vehicles for Chinese espionage? Are there any Chinese firms that you believe are flying under the radar in terms of dominating strategically important industries?

**A.1.** Several of the recommendations made by The U.S.–China Economic and Security Review Commission in 2019 spotlight the need for greater regulation and transparency of Chinese involvement in the U.S. financial system, including the role of the Chinese Communist Party (CCP) in businesses operating in the United States.

As we've seen from companies like Build Your Dreams (BYD) and the China Rail Rolling Stock Corporation (CRRC), these companies are eager to conceal their connections to the CCP as they endeavor to undermine American manufacturers. Already one of the world's largest battery producers and the world's largest electric vehicle company, BYD executives have been outspoken in their plans to one day sell passenger electric vehicles in the United States. In 2008, BYD's chairman has "boasted of plans to dominate world auto sales by 2025" and, more recently, a BYD executive said the company planned to sell passenger cars in the United States in "roughly 2 to 3 years." Left unchecked, BYD's business model would threaten over 5,600 auto parts suppliers spread across the Nation, employing 871,000 workers.

On March 29th BYD announced that it will start offering a full suite of EV components to rivals and aspiring auto manufacturers to diversify its revenue sources amid sputtering car demand.

Among the parts that the Shenzhen-based company makes and now sells are electric-car batteries, powertrains, and lights. BYD will use the brand name FinDreams for the parts business.

Beyond CRRC and BYD, there are several other industries Congress should consider as potential vehicles for Chinese espionage and several Congress should take a closer look at in terms of strategically important industries where China has an outsized influence.

*Port Logistics IT Systems.* China is exporting a global logistics information network in order to govern, collect information on, and shape global resource flows and data. Chinese leaders argue that their network will give them both market advantages over the United States and coercive leverage. China's approach nests within a broader competitive strategy. Careful consideration should be given to any potential proliferation of Chinese-owned, -administered, or -accessible logistics information networks to U.S. critical

infrastructure. Beijing's approach to these systems poses credible security and economic threats.

*Telecom Networks.* U.S. security and foreign policy officials have long voiced grave concerns that Huawei's 5G network would compromise confidential information, arguing that Huawei is ultimately obligated to serve the Chinese Communist Party (CCP). Last year, Secretary of State Michael Pompeo penned an opinion for POLITICO, stating, "With 5G capabilities, the CCP could use Huawei or ZTE's access to steal private or proprietary information, or use 'kill switches' to disrupt critical future applications like electrical grids and telesurgery centers. And one only needs to look at the CCP's extensive human rights abuses in Xinjiang—so clearly laid out in recently leaked documents—to see how it is using technology for mass repression."

Though Huawei contends that it is a private company and has not received any special treatment from the Chinese Government, it is estimated that Beijing substantially subsidizes the company, having provided \$75 billion in State support. Despite public relations campaigns, suspiciously modeled after typical CCP techniques, that recast Huawei as simply another tech company, research has revealed employee links between Huawei and China's military and intelligence services. Furthermore, as the *Wall Street Journal* exposed this summer, Huawei technicians have already enabled Governments in Africa to access information, including encrypted communications, to spy on political opponents.

*Minerals.* Minerals are essential to manufacturing components for everything from electric vehicles, smartphones, medical screening to weapons systems used by the military. But the United States remains heavily dependent on foreign sources for many of its critical minerals. About 91 percent of the rare earth element needed to make night-vision goggles for the military, for example, is imported from China.

In 2017, President Trump issued an executive order to address these vulnerabilities, tasking the Interior Department with developing a list of critical minerals and the Commerce Department with devising a strategy—including action plans, goals, and recommendations—to secure vital supply chains here in the United States. The Interior Department released its report in 2018, finding that 31 of the 35 minerals designated as "critical" are import-reliant. The U.S. doesn't have any domestic production and relies completely on imports for 14 critical minerals, the Interior Department found. Commerce followed up with its action plan in June 2019. Twenty-four goals and 61 specific recommendations were issued, including implementing better mineral recycling programs; developing technological alternatives to minerals; source diversification; improving processes for mineral extraction; building robust manufacturing capabilities; and enhancing minerals trade with America's allies.

But of course, doing all this is easier said than done—and in the meantime, the United States remains dependent on countries like China and Russia for its critical minerals. China began scaling up mining capabilities of rare earth elements in the 1980s, resulting in their near-monopoly on both the mining of rare earth minerals and the processing of the resultant rare earth oxides into manufac-

tured products. China's market power over rare earths now poses a national defense threat. China can quickly create a supply shock; their global market can respond by reducing demand and developing their own mining and processing capacities. There's no doubt that the U.S. is reliant on China. Between 2014 and 2017, 80 percent of rare earth element imports came from China, while the remaining 20 percent was originally processed in China.

*Pharmaceuticals.* The U.S.–China Economic and Security Review Commission calls for Congress to address U.S. dependence on Chinese pharmaceuticals. The Commission's 2019 report recommends that Congress continue to hold hearings exploring U.S. dependence on China's pharmaceuticals. However, the commission is clear on the goal of these hearings: Legislation that requires the Food and Drug Administration to identify pharmaceuticals that are manufactured exclusively in China or formulated with the active pharmaceutical ingredients made in China, as well as an investigation to determine whether those drugs are manufactured with as much regulation as pharmaceuticals produced in America.

*Higher Education.* The U.S.–China Economic and Security Review Commission calls for Congress to mandate the creation of a higher education advisory board comprised of representatives from universities and relevant Federal agencies. This board, which would be established within the Federal Bureau of Investigation (FBI), would aim to secure the American academic research system from espionage. This is already a focus of the FBI, which has been alerting academics of possible vulnerabilities as instances of academic espionage accumulate. An outsize number of these cases involve pilfered research being funneled to China.

Given that China appears to blend the its militarily and civilian sectors in the service of a common political objective set by the Chinese Communist Party (CCP), would the United States be unreasonable to view powerful Chinese commercial firms as extensions and enablers of the Chinese military, and as instruments of the CCP?

It would not be unreasonable for the U.S. to view Chinese Commercial firms as extensions of the Chinese military and as instruments of the CCP. As the U.S.–China Economic and Security Review Commission has noted, "some private Chinese companies operating in strategic sectors are private only in name, with the Chinese Government using an array of measures, including financial support and other incentives, as well as coercion, to influence private business decisions and achieve State goals."

For example, CRRC is Beijing's national champion in rail and emerging transportation systems. It plays a direct role in China's military–civil fusion strategy. According to research released by Radarlock in 2019, CRRC is working directly with Beijing to obtain foreign technology, collect sensitive data, and export technologies and information systems that threaten individual and data security, including those of Huawei. CRRC executives wear "dual hats" as corporate and Party leaders, appointed for political purposes.<sup>1</sup>

<sup>1</sup>"CRRC and Beijing's Dash for Global Rolling Stock Dominance", Bruyere and Picarsic. Radarlock. October 2019.

As another example, BYD uses its status as a “private company” to “obtain technology, information, and positioning from the international market, then to carry those back to the CCP and the People’s Liberation Army (PLA).” Meanwhile, its research and development centers are “incubated” in military–civil fusion zones that focus on technology transfer and data sharing. BYD and now-banned Huawei signed a “comprehensive strategic cooperation agreement” in March 2019, solidifying a long-standing, “inseparable” partnership between the two firms. BYD not only benefits from the Made in China 2025 strategy, it is helping to formulate the next iteration: China Standards 2035.<sup>2</sup> This paints a troubling profile of a company with deep ties to the Chinese Government and military that is trying to masquerade as a commercial entity.

Several of the recommendations made by The U.S.–China Economic and Security Review Commission in 2019 spotlight the need for greater regulation and transparency of Chinese involvement in the U.S. financial system, including the role of the Chinese Communist Party (CCP) in businesses operating in the United States.

It is also apparent that China is attempting to establish global information and standard-setting dominance by infiltrating little known standard-setting bodies to gain advantages. How could the U.S. dramatically raise China’s cost of executing its current strategy?

China is exporting a global logistics information network in order to govern, collect information on, and shape global resource flows and data. Chinese leaders argue that their network will give them both market advantages over the U.S. and coercive leverage. China’s approach nests within a broader competitive strategy. Careful consideration should be given to any potential proliferation of Chinese-owned, -administered, or -accessible logistics information networks to U.S. critical infrastructure. Beijing’s approach to these systems poses credible security and economic threats.

Beijing’s network encompasses logistics information systems, logistics standards systems, logistics policies, and logistics operating systems. Those extend across railways, roads, air, shipping, pipelines, postal, warehousing, and international distribution networks. The Chinese National Transportation Logistics Information Sharing Platform and suite of corresponding port software systems offer a concrete example of Beijing’s maneuvering. Through those Ministry of Transport-controlled tools, China collects and disseminates ratings data (e.g., on individuals, companies, vehicles); tracking data (e.g., on vehicles, cargo, customs clearance); resource data (e.g., price indexes, route planning, supply chains); and so-called “comprehensive data” (e.g., on policies and regulations, standards, interconnection between companies and infrastructures and softwares). Already more than 30 international ports have adopted the Chinese State-backed standard. More than 400,000 international shipping and logistics companies (including American ones) are connected to it.

Another important step would be to rethink the 2017 Federal Retirement Thrift Investment Board (FRTIB) decision to switch the

<sup>2</sup>“Building the China Dream: BYD & China’s Grand Strategic Offensive”, Bruyere and Picaresic. Radarlock. October 2019.



benchmark for one of its investment funds to mirror an index with Chinese assets. Having a Federal retirement plan investing in Chinese companies will only lessen China's cost of executing its current strategy. This specific fund is worth around \$50 billion. The index in question is admittedly huge, with more than 2,000 companies from dozens of countries on it. Among the Chinese companies included are Hikvision, a surveillance equipment manufacturer that has been involved in China's ongoing crackdown on its Uighur minority population. It was blacklisted by the Trump administration, which essentially blocks it from buying product inputs from U.S. companies. Another is ZTE, the telecommunications firm that faced the blacklist last year for selling equipment to Iran and North Korea despite U.S. sanctions. There are others too, like a Chinese weapons-systems manufacturer that makes stealth fighters, and a Chinese cell phone company that the Federal Communications Commission blocked from facilitating international calls in the United States because of concerns over espionage.

Additionally, I would like to reiterate the policy steps from my testimony that the United States could use to dramatically raise China's cost of executing its current strategy:

*Implement the Transportation Infrastructure Vehicle Security Act (TIVSA) Without Further Delay.* An unacceptable amount of time has now passed since TIVSA enactment and the Administration has yet to notify or release guidance to transit agencies. We are concerned that failing to educate transit agencies in a timely manner about how TIVSA impacts their planning decisions leaves an opening for deception and misinformation.

*Defend and Enhance TIVSA.* Already, there are forces at work to undermine TIVSA. Shortly after enactment, CRRC held a "thank you" event at which speakers discussed plans to indefinitely extend the 2-year implementation delay.<sup>3</sup> We urge Congress to reject any attempts to undermine the TIVSA law. Instead, AAM supports efforts to accelerate implementation, educate transit agencies, and enhance the law.

*Tighten Buy America Laws.* AAM supports making improvements to longstanding Buy America laws by closing loopholes, modernizing rules for battery content, and adding additional teeth to prevent erosion of our supply chains. We find it concerning that companies like BYD are meeting the statutory Buy America threshold with electric batteries assembled domestically almost entirely of foreign content, with little to no domestic processing in the United States. It is appropriate, in our view, to recognize that short-term market limitations exist in battery cell production and create a Buy America framework for electric batteries that rewards value added by American workers. We must also ensure that other non-battery components and parts continue to be produced in the United States and are not diminished by virtue of the outsized cost of the electric battery.

*Develop a Policy Framework for Domestic Battery Production.* Faced with a deeply distorted global market, Congress and the Administration should work together to establish a mix of incentives

<sup>3</sup>"CRRC MA, Rep. Richard Neal Celebrate Victory in Washington; Compromise Allows Rail Car Company To Keep Seeking New Work", Jim Kinney. *MassLive*. 23 December 2019.

and policies that maximize the utilization of new energy vehicles and expand the supply chain for the domestic production of electric batteries and battery cells.

*Conduct Buy America Audits.* AAM encourages further scrutiny of both CRRC's and BYD's Buy America certifications to ensure compliance. Both companies appear to rely heavily on imported Chinese content and the Albuquerque IG report raised significant questions as to the legitimacy of BYD's certification.

*Invest in America's Failing Infrastructure.* Last, but certainly not least, we encourage you to continue the challenging work of passing a substantial infrastructure investment paired with strong Buy America requirements.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN  
FROM SCOTT N. PAUL**

**Q.1.** In your testimony, you stated that “CRRC rapid ascent raises alarming questions about Beijing’s backdoor access to and operational control over critical technology embedded in our rail infrastructure—such as GPS, sensors and other safety features.” And that “this was a clear statement that Beijing should not have operational control of or access to a major U.S. transit system, opening our critical infrastructure to potential attack or backdoor access to sensitive data and communications of riders.” In cybersecurity terms, a backdoor is an undocumented method of bypassing security controls to covertly access a computer system or encrypted data. The cybersecurity firm Cybereason revealed mobile phone networks across the globe had been infiltrated over a 6-year period using techniques commonly associated with Chinese threat actors.

Currently, rolling stock is purchased with hardware and software bundled from the same manufacture. Do you believe that domestic cybersecurity would be improved if the DOT prohibited the bundling of hardware and software from the same manufacture and instead required an architecture that would allow other manufactures to provide alternative hardware and/or software options for rolling stock?

**A.1.** This is not an area of expertise for AAM, but it is certainly an issue that deserves more attention and action. A blanket prohibition of bundling hardware and software from the same manufacturer could have unintended consequences, and it may be worthwhile to establish protocols to allow for review on a case by case basis. Whatever the policy outcome, we must ensure that it is guided by promoting competition from trusted sources, is measured with stringent, universal, enforceable standards, and is able to evolve to meet the demands of both current and new threats that will arise.

What we do know is that CRRC is Beijing’s national champion in rail and emerging transportation systems and there should be no role for it in our public transportation system, regardless of any improvements we can make to cybersecurity protocols. CRRC plays a direct role in China’s military–civil fusion strategy. According to research released by Radarlock in 2019, CRRC is working directly with Beijing to obtain foreign technology, collect sensitive data, and

export technologies and information systems that threaten individual and data security, including those of Huawei.<sup>1</sup>

**Q.2.** Do you support the Federal Government funding software and hardware substitutes for potentially vulnerable transportation and other critical infrastructure?

**A.2.** Far too many new products are developed in America with Federal research and development funding only to be produced abroad. We encourage Congress to prioritize and support software and hardware substitutes, but we must match that pledge with testing support and other policies to ensure that the next breakthrough is made here by American workers. And, it goes without saying, but we must ensure that any entities receiving Federal support do not have ties to China's Government, military, or bad actors like Huawei.

**Q.3.** Policymakers often discuss mitigating cybersecurity attacks in terms improving cyberdefenses, but another method to combat State-sponsored cyberattacks would be to enact strong deterrents. Which specific deterrents do you believe would be effective against potential Chinese State-sponsored cyberattacks?

**A.3.** Several of the recommendations made by The U.S.–China Economic and Security Review Commission in 2019 spotlight the need for greater regulation and transparency of Chinese involvement in the U.S. financial system, including the role of the Chinese Communist Party (CCP) in businesses operating in the United States.

Implementing the Transportation Infrastructure Vehicle Security Act (TIVSA) without further delay, would be one effective deterrent. An unacceptable amount of time has now passed since TIVSA enactment and the Administration has yet to notify or release guidance to transit agencies. We are concerned that failing to educate transit agencies in a timely manner about how TIVSA impacts their planning decisions leaves an opening for deception and misinformation.

Defending and enhancing TIVSA is another. Already, there are forces at work to undermine TIVSA. Shortly after enactment, CRRRC held a “thank you” event at which speakers discussed plans to indefinitely extend the 2-year implementation delay. We urge Congress to reject any attempts to undermine the TIVSA law. Instead, AAM supports efforts to accelerate implementation, educate transit agencies, and enhance the law.

Having a robust domestic industry that can be agile in addressing the changing landscape in this area is also important. AAM supports making improvements to longstanding Buy America laws by closing loopholes, modernizing rules for battery content, and adding additional teeth to prevent erosion of our supply chains. We find it concerning that companies like BYD are meeting the statutory Buy America threshold with electric batteries assembled domestically almost entirely of foreign content, with little to no domestic processing in the United States. It is appropriate, in our view, to recognize that short-term market limitations exist in battery cell production and create a Buy America framework for elec-

<sup>1</sup>“CRRRC and Beijing’s Dash for Global Rolling Stock Dominance”, Bruyere and Picarsic. Radarlock. October 2019.

tric batteries that rewards value added by American workers. We must also ensure that other non-battery components and parts continue to be produced in the United States and are not diminished by virtue of the outsized cost of the electric battery. Beyond improving on Buy America, the United States must conduct Buy America audits. AAM encourages further scrutiny of both CRRC's and BYD's Buy America certifications to ensure compliance. Both companies appear to rely heavily on imported Chinese content and the Albuquerque IG report raised significant questions as to the legitimacy of BYD's certification.

Another, important step would be to rethink the 2017 Federal Retirement Thrift Investment Board (FRTIB) decision to switch the benchmark for one of its investment funds to mirror an index with Chinese assets. Having a Federal retirement plan investing in Chinese companies that may have ties to the Chinese Communist Party (CCP) is not exactly a deterrent. This specific fund is worth around \$50 billion. The index in question is admittedly huge, with more than 2,000 companies from dozens of countries on it. Among the Chinese companies included is ZTE, the telecommunications firm that faced the blacklist last year for selling equipment to Iran and North Korea despite U.S. sanctions.

#### **RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON FROM EMILY DE LA BRUYERE**

**Q.1.** At the end of your submitted testimony, you stated that the United States is inadvertently “fueling” China’s bid to establish a global web of cross-domain dependency, offering NASA’s collaborative dialogue with China as an example. Could you expand upon that thought and describe in more detail the various ways in which the U.S. is unintentionally aiding China’s long-term strategic goals?

**A.1.** Beijing’s strategy rests on the weaponization of cooperation. China asymmetrically integrates into international partnerships, siphoning foreign resources and claiming global leverage without releasing its own resources or ceding leverage over system. This posture is codified in Chinese strategic thought as “two markets, two resources.”<sup>1</sup> the international market is to be penetrated while the domestic one is protected; foreign resources to be shared over international networks while domestic ones are held tightly at home.

NASA, and other examples of scientific and technological partnerships in strategic—especially dual use—domains bear this out: They grant China access to determinative resources that it converts into power. See BeiDou, China’s military–civil fusion champion, in the NASA case. But also see the spike in, unprotected, Government investment in basic artificial intelligence capabilities that followed China’s claims to be investing in the same, and Beijing’s ability to siphon the resultant fruits.

Through such partnerships, Beijing is also able to establish footholds in critical infrastructures and technologies that it can hold at

<sup>1</sup> Emily de La Bruyere and Nathan Picarsic, “Viral Moment: China’s Post-COVID Planning”, Horizon Advisory, March 15, 2020, <https://www.horizonadvisory.org/news/coronavirus-series-report-launch-viral-moment-chinas-post-covid-planning>.

risk: In the CRRC case, U.S. transportation systems; in the NASA case, space; in the emerging technological domain, learning datasets and autonomous car technology. Beijing also—and this is particularly relevant in the present COVID-19 crisis—actively games U.S. industrial policy for resources and leverage. Beijing used the 2008 and 2009 relief measures to carve out a place for its champions in U.S. infrastructure. It intends similarly to subvert U.S. responses to COVID-19.<sup>2</sup>

That is just the beginning. The step after parasitically benefiting from and coopting systems is to govern them. Beijing games the multilateral standard-setting bodies to which the U.S. grants it access (e.g., the World Trade Organization, ICANN, the International Telecommunications Union). In those, Beijing deploys scale, regulatory arbitrage, and control over its State-directed champions to set global rules according to its interests. Less formally, it does the same with its leverage over the U.S. financial system (whether Wall Street or pension funds), U.S. universities, and U.S. media.

**Q.2.** What other industries should Congress consider as potential vehicles for Chinese espionage? Are there any Chinese firms that you believe are flying under the radar in terms of dominating strategically important industries?

**A.2.** Beijing prioritizes less by industry sector more by industry type. It focuses on coopting international networks, standards, and platforms. According to that logic, particular priority areas include: Transportation infrastructure (e.g., rail, sea, autonomous, and new-energy vehicles), critical supply chains (e.g., pharmaceuticals, batteries, advanced manufacturing, microelectronics), space, next-generation information infrastructure (e.g., communications, surveillance), 5G and Internet protocols, FinTech, critical datasets (e.g., for defense applications, precision agriculture), logistics.

All of these domains have their champions. Beijing calls its strategy “Government-directed, enterprise-driven.” Well-known names figure: Huawei in telecommunications, LOGINK<sup>3</sup> in logistics, DJI in autonomous systems, AliPay in FinTech. But there is a larger infrastructure below and around them as well—of other Chinese champions, but also of Chinese investment funds and investors who coopt foreign players to act in Beijing’s interest.

All are indeed flying under the radar. Until we have documentation and an information portal for interagency Federal Government access and Federal-State-local information sharing on Chinese companies, capital, and standard-setting systems, they will continue to do so.

**Q.3.** Given that China appears to blend the its militarily and civilian sectors in the service of a common political objective set by the Chinese Communist Party (CCP), would the United States be unreasonable to view powerful Chinese commercial firms as extensions and enablers of the Chinese military, and as instruments of the CCP?

**A.3.** This would not be unreasonable. It would be factual. Beijing’s military-civil fusion strategy codifies that military and civilian sec-

<sup>2</sup>Ibid.

<sup>3</sup>See Horizon Advisory’s forthcoming report on China Standards 2035 and LOGINK due to be released April 2020 at [www.chinastandards2035.com](http://www.chinastandards2035.com) and [www.horizonadvisory.org](http://www.horizonadvisory.org).

tors serve a common, Chinese Communist Party objective; that Chinese commercial firms enable Beijing's military and Party interests. A 2013, Chinese definition of the military-civil fusion strategy emphasizes as much: "The military is for civilian use, the civilian is military, and the military and civilian are fused."<sup>4</sup> This does not just mean that Chinese commercial champions enable Beijing's military ambitions and serve as CCP instruments. It also means that Chinese capital does.

**Q.4.** It is also apparent that China is attempting to establish global information and standard-setting dominance by infiltrating little known standard-setting bodies to gain advantages. How could the U.S. dramatically raise China's cost of executing its current strategy?

**A.4.** First, the U.S. needs actively to compete. It needs to recognize the strategic value of standard-setting bodies, and fight for its interests in them. Beijing has a national strategy for deploying its representatives at 3GPP (the industry group that sets 5G standards). The U.S. should too.

Second, China subverts international bodies precisely by breaking their rules: It benefits from the advantages of the WTO without complying with its most basic requirements. The U.S. should use its leadership position in these bodies to make them hold China accountable. It should make them do their most basic job: Enforce the rules.

Where that is not possible, the U.S. should be prepared to build alternative systems. Where Beijing has subverted the existing order so that it threatens U.S. strategic maneuver, Washington should not be afraid to abandon subverted institutions—and to create alternatives in tandem with its trusted allies. Just as Beijing threatens to establish a parallel WHO for leverage and manipulation, Washington needs to be open to disrupting the systems China has coopted.

---

#### RESPONSES TO WRITTEN QUESTIONS OF SENATOR COTTON FROM FRANK J. CILLUFFO

**Q.1.** What other industries should Congress consider as potential vehicles for Chinese espionage? Are there any Chinese firms that you believe are flying under the radar in terms of dominating strategically important industries?

**A.1.** Virtually all industries are potential targets and vehicles for Chinese espionage. From agriculture to aeronautics and beyond, China has demonstrated both sophistication and persistence in its efforts to breach the systems and networks of U.S. industry. The Made in China 2025 strategy, a key plank in China's drive for strategic dominance, is powered by Chinese espionage and represents a top priority of China's political leadership. This Strategy identifies ten key sectors: (1) next-generation information technology, (2)

---

<sup>4</sup>Emily de La Bruyere and Nathan Picarsic, "Military-Civil Fusion: China's Approach to R&D, Implications for Peacetime Competition, and Crafting a U.S. Strategy", 2019 USN/NPS Acquisition Research Symposium, May 2019; Emily de La Bruyere and Nathan Picarsic, "The Reach of China's Military-Civil Fusion: Coronavirus and Supply Chain Crises", *Real Clear Defense*, March 4, 2020, <https://www.realcleardefense.com/articles/2020/03/04/the-reach-of-chinas-military-civil-fusion-coronavirus-and-supply-chain-crises-115092.html>.

high-end numerical control machinery and robotics, (3) aerospace and aviation equipment, (4) maritime engineering equipment and hightech maritime vessel manufacturing, (5) advanced rail equipment, (6) energy-saving and new energy vehicles, (7) electrical equipment, (8) agricultural machinery and equipment, (9) new materials, and (10) biopharmaceuticals and high-performance medical devices. (See listing in <https://fas.org/sgp/crs/row/IF10964.pdf>.)

In addition, China's inroads into key U.S. sectors such as transportation and telecommunications in turn provides China an entree into other crucial U.S. sectors, because transportation and telecommunications are the hubs that serve other critical spokes—including the U.S. military.

Other smaller but still important opportunities exist for China's State-owned enterprises to make inroads into U.S. critical infrastructure either directly or indirectly. Flush with the financial backing of their sponsor (China), these foreign proxy entities can step in and scoop up U.S. assets and entities that are on the verge of bankruptcy or in need of start-up capital. Even more concerning is the extent to which we don't know what we don't know, which speaks to the second part of your question. While some Chinese firms such as Huawei and ZTE have entered the national lexicon, others such as drone-maker DJI and (video surveillance) equipment manufacturer Hangzhou Hikvision Digital Technology are well known to the U.S. intelligence and law enforcement communities; but the bigger concern would be Chinese entities that have not yet come onto U.S. radar screens. Against this broader background, no U.S. industry sector is off limits.

**Q.2.** Given that China appears to blend its military and civilian sectors in the service of a common political objective set by the Chinese Communist Party (CCP), would the United States be unreasonable to view powerful Chinese commercial firms as extensions and enablers of the Chinese military, and as instruments of the CCP?

**A.2.** This view would not be unreasonable; quite the contrary actually. This is so not only because China blurs the lines between political party, civilian society, and the military; but also because Chinese law requires that Chinese commercial firms stand ready to assist the State. On the latter point, at least three instruments are at play: China's National Intelligence Law of 2017, the associated Implementing Regulations, and Communist Party requirements enshrined in law and iterated publicly in 2014, 2015, and 2017. In a nonmarket setting such as China, this means that firms could be invoked even unwittingly to assist and further State goals and objectives set by the country's political leaders and executed by the Chinese military as directed.

**Q.3.** It is also apparent that China is attempting to establish global information and standard-setting dominance by infiltrating little known standard-setting bodies to gain advantages. How could the U.S. dramatically raise China's cost of executing its current strategy?

**A.3.** According to the U.S. Cyberspace Solarium Commission (on which I served as a Commissioner), China is greatly outpacing the United States in terms of participation and spending on inter-

national governance fora, including standards-setting bodies. Academics have estimated that the budget for China's external propaganda is roughly \$10 billion annually. Some of this funding is spent on ensuring widespread participation and influence in these fora. In contrast, the U.S. Department of State spent \$666 million on public diplomacy in fiscal year 2014, with a correspondingly limited amount on participation in international fora. Additionally, Chinese nationals currently serve as the heads of four of the fifteen U.N. specialized agencies. The country with the next highest number of leadership positions is France, with two. No other country, the United States included, holds more than one leadership position.

The United States must take steps to counter China's dominance in these bodies. First, the U.S. must show up in these venues even though in the past these lesser-known fora may have been viewed as peripheral, or at least not central, entities. The recent victory by the Singaporean candidate for the position of Director General of the World Intellectual Property Organization (WIPO) was a sorely needed success story on this front. In this instance, the U.S. and its partners realized that China was on the cusp of gaining a fifth U.N. specialized agency leadership position. Such an outcome would be akin to allowing the fox to guard the henhouse. Fortunately, the U.S. and its allies were able to come to a consensus and collectively mobilize their diplomats to rally support for the Singaporean candidate. This type of cooperation highlights the United States' (continuing) ability to organize a successful effort to protect U.S. values in a high-stakes contest with China.

The recent WIPO success was not guaranteed and there is more that the U.S. can and must do to reinforce its position in these international fora, specifically in standards-setting bodies. To this end, the Cyberspace Solarium Commission recently recommended empowering and sufficiently resourcing the National Institute of Standards and Technology (NIST) to facilitate robust and integrated U.S. participation from the Federal Government, academia, professional societies, and industry, in fora that engage in setting information and communications technology standards. This participation would include not only technical and standards experts from the Federal Government, but also skilled diplomats. A more robust and integrated approach, between and among U.S. Government officials and U.S.- and Western-based businesses will allow the U.S. to more vigorously present an alternative and compelling position and vision in these venues, so as to expose the Chinese position for what it is: a power play that benefits China and China alone (with the possible exception of some other authoritarian Nation States that may share certain Chinese interests and values, such as keeping domestic populations in check by all means necessary).

The U.S. must work energetically with its existing allies—and seek to cultivate new ones—so as to defend/protect existing global standards that support and reflect U.S. interests and values, as well as further the elaboration of new global norms that are equally in keeping with our interests/values. Sustained U.S. leadership, exercised in the described manner, will go a long way towards thwarting China's bid for dominance in this area.



**RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARREN  
FROM FRANK J. CILLUFFO**

**Q.1.** In your testimony, you stated that “the potential for continuous and purposeful (adversary) access to our railcar/transit systems may arise through equipment communications links; hardware or software may be compromised; and the likelihood of direct access is real.”<sup>1</sup> In cybersecurity terms, a backdoor is an undocumented method of bypassing security controls to covertly access a computer system or encrypted data. The cybersecurity firm Cybereason revealed mobile phone networks across the globe had been infiltrated over a 6-year period using techniques commonly associated with Chinese threat actors.<sup>2</sup>

Currently, rolling stock is purchased with hardware and software bundled from the same manufacturer. Do you believe that domestic cybersecurity would be improved if the DOT prohibited the bundling of hardware and software from the same manufacture and instead required an architecture that would allow other manufacturers to provide alternative hardware and/or software options for rolling stock?

**A.1.** Diversification is often a prudent strategy and the proposed context is no exception to the extent that it makes little sense to introduce a potential single point of failure or vulnerability if there are other equally powerful paths forward. However acquiring unbundled hardware and software will not resolve the foundational issue in relation to Chinese-supplied rolling stock—namely, that any manufacturer must be tested/vetted and trusted by U.S. authorities before being allowed to infiltrate the supply chain of critical U.S. infrastructure (or critical national functions).

Having said that, it would nonetheless be good practice to adopt measures that enhance cybersecurity in the context of any and all trusted vendors, including American ones.

**Q.2.** Do you support the Federal Government funding software and hardware substitutes for potentially vulnerable transportation and other critical infrastructure?

**A.2.** As I stated in my previous answer, unbundled hardware and software will not resolve the foundational issue in relation to Chinese-supplied rolling stock—namely, that any manufacturer must be tested/vetted and trusted by U.S. authorities before being allowed to infiltrate the supply chain of critical U.S. infrastructure (or critical national functions).

However, while banning or limiting market access to “high-risk” vendors (like Huawei, ZTE, Hikvision, or others) can limit supply-chain vulnerabilities, without secure, cost-competitive substitutes, America’s own domestic infrastructure development may be slowed or stymied. The United States must take steps to build a stronger, more secure industrial base for critical materials, components, and technologies for critical infrastructure sectors where there is a growing dependence on China or untrusted vendors. This “industrial base strategy” should draw upon lessons from the past and

<sup>1</sup>Testimony of Frank J. Cilluffo, Director, Center for Cyber and Homeland Security Auburn University before the Banking Committee, March 3, 2020.

<sup>2</sup><https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers>

take a holistic approach, utilizing a “Sematech-like” model to spur domestic innovation and capacity. We should also look for opportunities to expand this model beyond our borders, leveraging the industrial might of our allies and partners to establish common, trusted foundries able to compete with and provide alternatives against insecure, State-backed Chinese products.

This also means the United States must take steps to consciously diversify its supply chains away from “concentrated dependencies” on any one foreign Nation. While a blanket “decoupling” from China would likely not serve U.S. interests, the United States must take stock of its most critical materials, components, and technologies and seek to provide incentives or subsidies for companies to move their manufacturing elsewhere. Geographic diversity in America’s global manufacturing base is critical in ensuring the resilience of supply in peacetime and in crisis. The Cyberspace Solarium Commission highlighted the need for this sort of industrial strategy to preserve U.S. resilience in IT hardware and software capabilities.

Bottom line: the United States must invest heavily to build domestic markets and manufacturing capabilities in critical areas; and should work to encourage our Five Eyes partners and other U.S. allies to invest accordingly as well.

**Q.3.** Policymakers often discuss mitigating cybersecurity attacks in terms improving cyberdefenses, but another method to combat State-sponsored cyberattacks would be to enact strong deterrents. Which specific deterrents do you believe would be effective against potential Chinese State-sponsored cyberattacks?

**A.3.** An effective deterrent strategy in cyberspace requires a strong defense working in tandem with other elements of national power. The Cyberspace Solarium Commission recently put forward a strategy termed “layered cyberdeterrence” to reduce the frequency, scope, and scale of adversary malicious cyberoperations. This strategy is composed of three layers. Shape behavior: the United States must work with allies and partners to promote responsible behavior in cyberspace. Deny benefits: the United States must deny benefits to adversaries who have long exploited cyberspace—to their advantage, to American disadvantage, and at little cost to themselves—by securing critical U.S. networks in collaboration with the private sector to promote national resilience and increase the security of the cyberecosystem. Impose costs: the United States must maintain the capability, capacity, and credibility needed, in all instruments of national power, to retaliate against actors who target America in and through cyberspace.

The Solarium Commission assessed that deterrence was not working in cyberspace, and that significant investment is needed in all three areas, but especially in the deterrence-by-denial layer. To this end, significant U.S. investment is needed in the defense and security of our national critical infrastructure—much of which is owned and operated by the private sector. The concomitant need for public–private collaboration presents a further challenge as we try to build/enhance effective deterrent capability.

As your question implies, deterrence must be tailored to the specific actor whose behavior the United States seeks to change. All

three of the enumerated layers are required to deter Chinese aggression in cyberspace.

In the case of China, we must marshal all elements of statecraft—economic, political, diplomatic, military, law enforcement, intelligence, and so on—in order to change the Chinese decision-making calculus. Accordingly, attribution, indictments, sanctions, joint and concerted action with allies, declaratory statements backed up by demonstrated abilities and capacities plus a willingness to act—all of these are important elements in the U.S. toolkit and should be invoked as circumstances warrant. Lashing up ever more tightly the efforts of the FBI, NSA, DOD, and DHS to better support U.S. critical infrastructure and critical national functions will also serve to deter in a more effective way than ever before, particularly if a more forward-leaning posture is adopted.

---

**RESPONSES TO WRITTEN QUESTIONS OF SENATOR SINEMA  
FROM FRANK J. CILLUFFO**

**Q.1.** What are the threats to American passengers riding on a China Railway Rolling Stock Corporation railcar with Huawei technology operating in the U.S.?

**A.1.** At the high end of the spectrum of potential concerns is disruptive or destructive action. In this regard, the threat centers on the potential for continuous and purposeful (adversary) access to our railcar/transit systems through equipment communications links (hardware or software may be compromised); and some of the consequences that could follow: China could shut down U.S. trains and disrupt transit operations. Knock-on effects could hit other critical U.S. infrastructure sectors. Major U.S. cities that depend strongly on rapid transit systems could experience significant economic effects, particularly if an incident were to disrupt systems for a lengthy period. In addition, China could engage in espionage that affects not just systems and infrastructures, but individual Americans (however there are many easier ways for China to pursue this particular end). Huawei having an additional “foothold” in the manner set out in your question would compound the situation (negatively).

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD  
**STATEMENT FROM PORTLAND CEMENT ASSOCIATION**



**Portland Cement Association**  
 200 Massachusetts Ave NW, Suite 200  
 Washington D.C. 20001  
 202.408.9494 Fax: 202.408.0877  
[www.cement.org](http://www.cement.org)

March 6, 2020 2020

The Honorable Michael Crapo  
 Chairman  
 Banking Committee  
 Washington, D.C. 20510

The Honorable Sherrod Brown  
 Ranking Member  
 Banking Committee  
 Washington, D.C. 20510

RE: Statement for the record of the Senate Banking Committee hearing on "Surface Transportation Reauthorization: Public Transportation Stakeholders' Perspectives"

Dear Chairman Crapo and Ranking Member Brown:

The Portland Cement Association appreciates the opportunity to submit this statement for the record for the committee's hearing "*Surface Transportation Reauthorization: Public Transportation Stakeholders' Perspectives*". This hearing is timely as Congress works to pass the next surface transportation authorization.

The Portland Cement Association (PCA) is the premier policy, research, education, and market intelligence organization serving America's cement manufacturers. PCA members represent 92 percent of the United States' cement manufacturing production capacity and have distribution facilities in every state in the continental United States. Cement and concrete product manufacturing, directly and indirectly, employs approximately 610,000 people across the country, and our collective industries contribute over \$125 billion to our economy. PCA promotes safety, sustainability, and innovation in all aspects of construction, fosters continuous improvement in cement manufacturing and distribution, and promotes economic growth and sound infrastructure investment.

Concrete forms when portland cement is mixed with water and aggregate (sand and rock) and allowed to harden. Cement holds the concrete together and has a similar role to flour in cake mix. Annually, the United States uses approximately 260 million cubic yards of concrete to build and repair a variety of different types of transportation and infrastructure, including public transit systems.

Efficient and well-functioning transit is an essential component of the nation's multimodal transportation system. Public transportation not only spurs economic growth, but also reduces congestion, improves air quality, and saves time and money. Transit ridership continues to grow in the United States. Between 1995 and 2018, public transit ridership grew by 27 percent surpassing U.S. population growth, which grew by 23 percent. Over this same period, passenger miles traveled on public transportation grew by 39 percent. These numbers demonstrate the critical role transit plays as a mode of transportation. Communities across the country can relate to the need for greater investment in transit.

Not only is there a growth in transit ridership across the country, but there is a large maintenance backlog. The U.S. Department of Transportation's State of the Nation's Highways, Bridges, and Transit report released at the end of last estimates more than \$99 billion is needed to achieve a state of good repair of the nation's transit systems. This does not even include what is needed to build new or expand existing systems to meet growing demand. Addressing the backlog in maintenance and expanding transit opportunities is needed to continue growth in ridership of transit systems across the country.



**Portland Cement Association**  
 200 Massachusetts Ave NW, Suite 200  
 Washington D.C., 20001  
 202.408.9494 Fax: 202.408.0877  
[www.cement.org](http://www.cement.org)

Reauthorization of the surface transportation program must finally address the long-term solvency of the Highway Trust Fund. The Congressional Budget Office's (CBO) annual Budget and Economic Outlook released in January, estimates that the Mass Transit Account will face a \$235 million shortfall in Fiscal Year 2021. CBO's new estimates for the Highway Trust Fund predict the ten-year insolvency of Mass Transit Account to be \$54.1 billion. CBO projects that total tax receipts at current rates will be \$426 billion over ten years, meaning to pass a long-term reauthorization of the highway and transit programs at current investment levels, the Highway Trust Fund will need an additional \$193 billion just to maintain current funding levels plus inflation. These numbers demonstrate the dire need for Congress to address the long-term solvency of the Highway Trust Fund.

In 2018, 44 transit and multimodal ballot measures increasing investment in transit were passed by communities across the United States. We cannot leave it to states and communities alone to increase investment in transportation. PCA supports an immediate 25 cent increase in the motor fuels taxes, indexed to inflation. Additional options should be considered in addition to increasing the gas tax – like transitioning to a national Vehicle Mile Travelled fee - to not only address the existing shortfall in funding but to raise enough revenue to help states and communities build the needed transportation infrastructure to meet anticipated future demands on the system.

Critical to helping communities meet the growing demand for transit across the country is the Capital Investment Grant (CIG) program. CIG provides funding to help communities build new and expand existing subways, light rail, commuter rail, streetcars, and bus rapid transit systems. There are currently 12 transit projects with full funding grant agreements and 50 more Capital Investment Grants projects are in the Federal Transit Administration's pipeline, requesting approximately \$25 billion of CIG funding in the coming years. Reauthorization should take steps to streamline the process for communities to apply and utilize the CIG program.

PCA appreciates the opportunity to share our members perspective that reauthorization of the FAST Act needs to increase investment in transit to enable communities to both address the growing maintenance backlog, expand existing systems, and help build new systems to meet the demand for transit across the country. We look forward to working with the committee and your colleagues in a bipartisan way to enact a long-term transportation reauthorization.

Sincerely,

A handwritten signature in black ink that reads 'Sean O'Neill'. The signature is written in a cursive, flowing style.

Sean O'Neill  
 Senior Vice President, Government Affairs  
 Portland Cement Association

## LETTER FROM RAIL SECURITY ALLIANCE



March 5, 2020

The Honorable Mike Crapo  
Chairman  
U.S. Senate Committee on Banking, Housing,  
and Urban Development  
534 Dirksen Senate Office Building  
Washington DC, 20510

The Honorable Sherrod Brown  
Ranking Member  
U.S. Senate Committee on Banking, Housing,  
and Urban Development  
534 Dirksen Senate Office Building  
Washington DC, 20510

Dear Chairman Crapo and Ranking Member Brown:

The Rail Security Alliance applauds your leadership in convening the Senate Banking, Housing, and Urban Affairs Committee hearing titled, "Threats Posed by State-Owned and State-Supported Enterprises to Public Transportation."

The topic of the hearing remains timely and is vital to both the economic and national security interests of the United States. We appreciate the opportunity to communicate to you the work of the Rail Security Alliance and the importance of further protecting the United States from Chinese state-owned enterprises.

**Who We Are:**

The Rail Security Alliance is a coalition of North American rail manufacturers, suppliers, unions, and steel interests that is committed to ensuring the economic and national security of passenger and freight rail systems. This alliance was formed in response to the merging of China's two rail manufacturers into one massive state-owned enterprise, the China Railroad Rolling Stock Corporation (CRRC).

CRRC, by their own calculation, controls roughly 83 percent of the global rail market. As a state-owned enterprise, CRRC has access to unlimited state funding that allows them to win contracts around the world by underbidding every other competitor, jeopardizing the future of this industry.

**The Threat from China:**

Over the past five years, the Chinese state-owned enterprise China Railway Rolling Stock Corporation (CRRC) has aggressively targeted the U.S. market as a means of advancing China's "Made in China 2025" initiative, which aims to overtake the United States and other nations in critical industries like passenger and freight railcar manufacturing. Using state-backed financing and other anti-competitive tactics, CRRC has now secured \$2.6 billion in contracts to build metro transit cars for Boston, Chicago, Philadelphia, and Los Angeles, sometimes underbidding its competitors by as much as several hundred million dollars.

It is not just about unfair financing; the broader implications of CRRC operating in the United States impact our national security. CRRC's bylaws direct that the company seek guidance from the Communist Party of China on significant matters affecting the company's operations. From IP theft to fears about spying on American citizens, the risks are real and alarming.

Congressional Action:

Congress, unsettled by these contracts and the unfair practices being used by CRRC, passed the Transit Infrastructure Vehicle Security Act (TIVSA) as part of the Fiscal Year 2020 National Defense Authorization Act, which was signed into law by President Trump in December of 2019. TIVSA blocks transit agencies from using American taxpayer dollars to procure transit rollingstock, railcars and buses, from Chinese state-owned enterprises and other entities that are Chinese state directed. It also permanently blocks the Washington Metro Area Transit Authority (WMATA) from ever procuring cars from CRRC.

TIVSA was a necessary policy fix, according to a June 2019 Oxford Economics study, for each job created by a Chinese SOE in the rail sector, the United States loses between 3.5 to 5.4 net jobs which factors out to a net loss of over 5,000 U.S. jobs for every \$1 billion won in contracts by China. CRRC should not be able to hide under the umbrella of American job creation while putting hardworking Americans out of work with our own taxpayer dollars. For this reason, we commend you both, alongside today's witnesses Senators Cornyn and Baldwin, for taking the necessary steps to curb unfair Chinese practices into the transit sectors of the United States.

We also want to take an opportunity to extend our sincere thanks for the passage of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA.) This legislation gave the Committee on Foreign Investment in the United States the updated tools it needed to combat predatory governments in the modern era, including tools necessary for CFIUS to examine the impacts of investments into U.S. critical infrastructure.

The Future of TIVSA and the Rail Industry in the United States:

We strongly encourage the Department of Transportation to implement TIVSA immediately to the fullest extent of its power and implore this committee, and the broader United States Congress, to continue to take the threat of Chinese state-owned enterprise seriously by protecting the integrity of TIVSA.

Only a few short months ago, CRRC MA, the Springfield, Massachusetts facility of CRRC, held a victory party to celebrate the two-year delay that was part of TIVSA. Many speaking at the event discussed the need to overturn the law – we cannot let that happen.

We appreciate all you have done to protect the rail industry in the United States and stand available to answer any questions.

Sincerely,



Erik Olson  
Vice President, Rail Security Alliance



## LETTER FROM SECURING AMERICA'S FUTURE ENERGY

SECURING AMERICA'S  
FUTURE ENERGY

1111 19<sup>TH</sup> STREET, NW  
SUITE 406  
WASHINGTON, DC 20036

TEL: 202-461-2360  
FAX: 202-461-2379  
SECUREENERGY.ORG



March 5, 2020

The Honorable Mike Crapo  
Chairman, Senate Committee on  
Banking, Housing, and Urban Affairs  
534 Dirksen Senate Office Building  
Washington, DC 20510

The Honorable Sherrod Brown  
Ranking Member, Senate Committee on  
Banking, Housing, and Urban Affairs  
534 Dirksen Senate Office Building  
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

China has made capturing the electric vehicle (EV) sector a central part of its Made in China 2025 strategy, through which China seeks to gain strategic advantages over global great-power rivals by dominating nascent critical industries. Beijing is pursuing this goal by, among other things, aggressively subsidizing Chinese companies, which enables them to underbid competitors to win business – clearly undermining principles of fair competition and competitive markets.

Securing America's Future Energy (SAFE) appreciates the opportunity to submit this letter for the hearing record. SAFE is a nonpartisan, nonprofit organization committed to reducing U.S. oil dependence to improve American economic and national security. In 2006, SAFE formed the Energy Security Leadership Council (ESLC), a nonpartisan group of business and former military leaders in support of long-term policy toward this goal. The ESLC is co-chaired by Frederick W. Smith, Chairman and CEO of FedEx, and General James T. Conway, 34th Commandant of the U.S. Marine Corps (Ret.). SAFE and its ESLC advocate for the use of EV technologies, among others, to bolster America's energy and national security, and we are increasingly concerned about China's use of Chinese-owned, controlled or subsidized companies to dominate markets, and thereby adversely affect U.S. industries.

China's growing dominance in the EV market threatens American competitiveness and has significant national security implications for the United States. The U.S. has leveraged its technological advantage to reduce its vulnerability to the Saudi-led, and Russia-allied, OPEC cartel. However, if we fail to address China's rising influence over the transportation sector, we will simply swap that vulnerability to OPEC and its allies for that to a Chinese-controlled EV supply chain – from minerals to markets. Moreover, the infiltration of Chinese technology into the EV sector raises substantial cybersecurity risks that may be difficult to assess and address. Taken together, we submit, and we are confident you agree, that is an untenable proposition for our nation's economic and national security.

At a May 16, 2019 House Transportation and Infrastructure Committee hearing, Democratic and Republican members alike expressed significant concerns with the Chinese government's subsidization of and support for companies engaged in the EV market, including support for companies with a U.S. presence. Chinese companies and the Chinese government are inexorably intertwined, which creates a host of economic and national security concerns for the United States.

Cognizant of this relationship, and under the leadership and support of Senators Cornyn and Baldwin and this Committee, Congress began addressing this problem with the introduction of the Transit Infrastructure Vehicle Security Act. This legislation would prohibit federal funds from being used by transit agencies to purchase buses and rail cars manufactured by companies that are wholly or in part



owned, controlled, or subsidized by the Chinese government. Congress then included this critical provision in the FY 2020 National Defense Authorization Act (NDAA), which was signed into law. SAFE applauds this Committee's work to continue to shine a spotlight on the threat posed by China's anticompetitive practices in this market.

The automotive industry has long been the backbone of America's industrial power, and domestic manufacturers are acutely aware of the implications of a global automotive industry heavily influenced, and perhaps dominated, by China. However, the threat extends beyond the vehicles themselves.

The U.S. government has largely ignored the emerging and accelerating dangers across the entire vehicle supply chain—from mineral extraction and processing, to battery production, to the design and assembly of vehicles.

The U.S. is deeply dependent on mineral imports from China. Today, U.S. companies must turn to imports to cover 92 percent of its lithium needs, 100 percent of its cobalt requirements, 59 percent of its nickel consumption, and 100 percent of graphite demand. These critical minerals, along with their rare earth counterparts, are critical to produce a variety of goods, ranging from EV batteries to precision-guided munitions for the Department of Defense.

While important first steps have been made to ensure American taxpayers are not indirectly funding Chinese state-owned and state-backed entities, a whole-of-government approach is needed to counter the broader threat of China's dominance over the mineral supply chain. While there is an increase in battery production facilities in the U.S., which is still insufficient for what is needed in the future, those manufacturers are still reliant on minerals mined and processed by China. Even if the U.S. were to scale up domestic extraction, China still maintains significant control over mineral processing facilities. This is an area of concern that extends beyond this Committee, but given your vital work on this issue, we hope to work with you and the rest of Congress in curbing China's ambition and thereby strengthening America's energy and national security.

The United States is the world's largest oil consumer, and our transportation system remains 92 percent reliant on petroleum fuels. A robust U.S. market for advanced fuel vehicles will not only provide greater consumer choice, but also create a long-term solution to the vulnerabilities posed by our dependence on oil.

SAFE supports the Committee's decision to continue to pay attention to this important issue, and we hope that the Committee members will continue to work with their colleagues to ensure the provision in the FY 2020 NDAA is fully implemented, and that Congress continues to address China's growing dominance in the EV sector. We look forward to continuing our work together to ensure America's competitiveness and security in the years to come.

Sincerely,



Robbie Diamond  
President and CEO  
Securing America's Future Energy

## LETTER FROM VIA METROPOLITAN TRANSIT



March 4, 2020

The Honorable Mike Crapo  
Chairman  
Senate Banking, Housing & Urban Affairs Committee  
534 Dirksen Senate Office Building  
Washington, D.C. 20510

The Honorable Sherrod Brown  
Ranking Member  
Senate Banking, Housing & Urban Affairs Committee  
534 Dirksen Senate Office Building  
Washington, D.C. 20510

**RE: Raising the small start net capital cost and federal assistance caps (49 U.S.C. § 5309(a)(7)) in surface transportation reauthorization legislation**

Dear Chairman Crapo and Ranking Member Brown:

On behalf of VIA Metropolitan Transit Authority, I write to encourage you to raise both the net capital cost cap and federal assistance cap for the Capital Investment Grant (CIG) small start program (49 U.S.C. § 5309(a)(7)) in the upcoming surface transportation reauthorization legislation. We request that the small start net capital cost cap be raised from \$300 million to \$400 million and the federal assistance cap be raised from \$100 million to \$200 million, allowing for up to 50% federal participation at the maximum cap, as opposed to 33% participation today.

Since 1964, Congress has provided funding to supplement and enhance certain local transit projects. The CIG program enables the Federal Transit Administration (FTA) to provide technical expertise to states, localities, and transit agencies as they work to improve transit options for their communities.

Most importantly, the CIG program also provides funding for fixed guideway investments – which are very much needed in the City of San Antonio and Bexar County. As the San Antonio region moves toward the expansion of transportation mobility options, the need for additional funding capacity and opportunities for both capital improvements and operations, is crucial. Since 2016, the public transportation provider in the region, VIA Metropolitan Transit Authority, has been advancing the development of rapid transit corridor projects, which would feature dedicated lanes for transit to provide the frequency and reliability needed to handle growth today and projected for tomorrow.

Throughout its existence, the CIG program has generated regional economic benefits, attracted businesses to project corridors, connected workers to job centers, and relieved congestion. The benefits of a project also extend well beyond the project corridor to manufacturing facilities across the United States. However, since the FAST Act was passed in 2015, cities and states are seeing higher transit project costs due to inflation, rising construction costs, and a tight labor market. Simply, the small start program's net capital cost cap and federal assistance cap has not been able to keep up with the intended purpose and without a modernization of the program in the next reauthorization period more and more projects will be artificially pushed into new starts when small starts would be the best fit.

Thank you for your consideration. We look forward to working with you to ensure that transit projects of all sizes have a strong federal partnership.

Sincerely,

Jeffrey C. Arndt  
President and CEO

VIA Metropolitan Transit  
123 N. Medina St. | San Antonio, Texas 78207 | (210) 299-5800  
VIAinfo.net