

**EMBEDDED THREATS: FOREIGN OWNERSHIP,
HIDDEN HARDWARE, AND LICENSING FAILURES
IN AMERICA'S TRANSPORTATION SYSTEMS**

HEARING
BEFORE THE
SUBCOMMITTEE ON OVERSIGHT
OF THE
COMMITTEE ON THE JUDICIARY
U.S. HOUSE OF REPRESENTATIVES
ONE HUNDRED NINETEENTH CONGRESS

SECOND SESSION

WEDNESDAY, JANUARY 21, 2026

Serial No. 119-52

Printed for the use of the Committee on the Judiciary



Available via: <http://judiciary.house.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2026

62-658

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California	JAMIE RASKIN, Maryland, <i>Ranking Member</i>
ANDY BIGGS, Arizona	JERROLD NADLER, New York
TOM McCLINTOCK, California	ZOE LOFGREN, California
THOMAS P. TIFFANY, Wisconsin	STEVE COHEN, Tennessee
THOMAS MASSIE, Kentucky	HENRY C. “HANK” JOHNSON, JR., Georgia
CHIP ROY, Texas	ERIC SWALWELL, California
SCOTT FITZGERALD, Wisconsin	TED LIEU, California
BEN CLINE, Virginia	PRAMILA JAYAPAL, Washington
LANCE GOODEN, Texas	J. LUIS CORREA, California
JEFFERSON VAN DREW, New Jersey	MARY GAY SCANLON, Pennsylvania
TROY E. NEHLS, Texas	JOE NEGUSE, Colorado
BARRY MOORE, Alabama	LUCY McBATH, Georgia
KEVIN KILEY, California	DEBORAH K. ROSS, North Carolina
HARRIET M. HAGEMAN, Wyoming	BECCA BALINT, Vermont
LAUREL M. LEE, Florida	JESÚS G. “CHUY” GARCÍA, Illinois
WESLEY HUNT, Texas	SYDNEY KAMLAGER-DOVE, California
RUSSELL FRY, South Carolina	JARED MOSKOWITZ, Florida
GLENN GROTHMAN, Wisconsin	DANIEL S. GOLDMAN, New York
BRAD KNOTT, North Carolina	JASMINE CROCKETT, Texas
MARK HARRIS, North Carolina	
ROBERT F. ONDER, JR., Missouri	
DEREK SCHMIDT, Kansas	
BRANDON GILL, Texas	
MICHAEL BAUMGARTNER, Washington	

SUBCOMMITTEE ON OVERSIGHT

JEFFERSON VAN DREW, New Jersey, *Chair*

BARRY MOORE, Alabama	JASMINE CROCKETT, Texas, <i>Ranking Member</i>
ROBERT F. ONDER, JR., Missouri	
DEREK SCHMIDT, Kansas	JARED MOSKOWITZ, Florida
BRANDON GILL, Texas	HENRY C. “HANK” JOHNSON, JR., Georgia

CHRISTOPHER HIXON, *Majority Staff Director*

ARTHUR EWENCZYK, *Minority Staff Director*

C O N T E N T S

WEDNESDAY, JANUARY 21, 2026

OPENING STATEMENTS

	Page
The Honorable Jefferson Van Drew, Chair of the Subcommittee on Oversight from the State of New Jersey	1
The Honorable Jasmine Crockett, Ranking Member of the Subcommittee on Oversight from the State of Texas	3
The Honorable Jamie Raskin, Ranking Member of the Committee on the Judiciary from the State of Maryland	4

WITNESSES

Emily de La Bruyère, Senior Fellow, Foundation for Defense of Democracies	
Oral Testimony	6
Prepared Testimony	9
Rocky Cole, Co-Founder, Chief Operating Officer, iVerify	
Oral Testimony	16
Prepared Testimony	19
Chris Spear, President, Chief Executive Officer, American Trucking Association	
Oral Testimony	22
Prepared Testimony	24
Rob K. Knake, Chief Executive Officer, TPO Group	
Oral Testimony	38
Prepared Testimony	40

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

All materials submitted for the record by the Committee on the Judiciary are listed below	59
An Interim Staff Report entitled, “The Weaponization of CISA: How a ‘Cybersecurity’ Agency Colluded with Big Tech and ‘Disinformation’ Partners To Censor Americans,” Jun. 26, 2023, <i>Committee on the Judiciary, Select Subcommittee on the Weaponization of the Federal Government</i> , submitted by the Honorable Brandon Gill, a Member of the Subcommittee on Oversight from the State of Texas, for the record	
Materials submitted by the Honorable Jasmine Crockett, Ranking Member of the Subcommittee on Oversight from the State of Texas, for the record	
An article entitled, “DOGE Put Critical Social Security Data at Risk, Whistle-Blower Says,” Aug. 26, 2025, <i>The New York Times</i>	
An article entitled, “Transportation Department targets 3,000 truck driving schools for non-compliance,” Dec. 1, 2025, <i>AP News</i>	

EMBEDDED THREATS: FOREIGN OWNERSHIP, HIDDEN HARDWARE, AND LICENSING FAILURES IN AMERICA'S TRANSPORTATION SYSTEMS

Wednesday, January 21, 2026

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON OVERSIGHT

COMMITTEE ON THE JUDICIARY

Washington, DC

The Committee met, pursuant to notice, at 2 p.m., in Room 2141, Rayburn House Office Building, the Hon. Jefferson Van Drew [Chair of the Subcommittee] presiding.

Members present: Representatives Van Drew, Onder, Gill, Crockett, Raskin, and Johnson.

Mr. VAN DREW. The Subcommittee will come to order. Without objection, the Chair is authorized to declare a recess at any time. We welcome everyone to today's hearing on foreign involvement and threats to America's transportation system.

I now recognize the doctor, the gentleman Dr. Onder from Missouri, to lead us in the Pledge of Allegiance.

ALL. I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation, under God, indivisible, with liberty and justice for all.

Mr. VAN DREW. Remain standing for a moment of silence.

I will now recognize myself for an opening statement. Again, I want to welcome everyone, and I want to thank the witnesses for being here today. I guess you could say this hearing is about control and who ultimately pays the price when we give that control away.

Every day, millions of Americans travel on our Nation's highways, leaving behind a detailed digital record of who they are, where they go, what their destination is, and how they got there. I want to say on this hearing today—and I may be wrong; we are going to find out there may be some bipartisanship, not on all the subjects of the hearing, but particularly on this piece of it. I am hopeful for that. We are going to find out. We all agree that this is a serious issue.

Electronic toll collection systems like E-ZPass were sold to the public as a convenience. You drive through; you get a bill later. Those bills get pretty big, by the way. Your data also does get

tracked. In an alarming trend, more and more of this data is being stored and being controlled by foreign entities.

In my home State of New Jersey, the E-ZPass system used by millions of residents—some of the most traveled roads in the United States of America are in the State of New Jersey, the New Jersey Turnpike, for example, used by millions and businesses as well, is now operated by a company under foreign government control, a Singaporean company with documented ties to the Chinese Communist Party.

That means Americans are paying tolls into a system that is not under American control. Interestingly enough, New Jersey had a choice. There was an American company that submitted a lower bid to operate the system. Many believed it was a responsible bid. Instead of choosing the option that would have kept control here at my home and save residents money, the State went with the higher, more expensive foreign bid.

This is at a time when families are struggling with inflation, high prices, and increased cost-of-living pressures. New Jersey taxpayers were asked to pay more for less accountability and less security. Higher costs, less transparency, more foreign control—it is a bad formula. The problems do not end with those who operate our toll systems. It extends to what is embedded inside the infrastructure itself.

The United States has become dangerously dependent on Chinese-manufactured infrastructure components, including batteries, sensors, and cameras. In 2024, the Department of Homeland Security estimated that at least—at least—12,000 Chinese-made internet cameras were already in use across United States infrastructure.

The February 2025 DHS report revealed that many of these cameras lack basic data encryption and security settings, and by default, they can communicate directly with their manufacturer located in China. That means foreign entities may have visibility into American facilities, American operations, and American vulnerabilities.

Chinese State-sponsored cyberattack groups linked to the Chinese Government have demonstrated the capability to infiltrate U.S. infrastructure, steal sensitive data, and maintain persistent access inside our networks.

Once again, it comes back to control. If we do not control the systems, the hardware, and the data, then we don't control the risk. The loss of American control does not stop with toll systems or infrastructure. Under the Biden Administration, States were allowed to issue CDLs, commercial driver licenses, to individuals who were not qualified and not proficient in English. This is where it may not be as bipartisan.

Truck drivers must be able to read road signs. If you are driving an 18-wheeler, a semi, on the road, you have to be able to understand the signs. I don't know why that is complicated. They have to be able to communicate with law enforcement and respond in emergencies. When States ignore those requirements, Americans pay the price.

Let me give you a few examples. On March 13, 2025, Austin, Texas, a tractor trailer driven—slowed for a stop in traffic plowed

into more than a dozen vehicles, killed five people, including an infant and a child. The driver couldn't read and write English. On November 14, 2025, Boone County, Indiana, an illegal immigrant from the country of Georgia driving with a New York-issued non-domiciled CDL lost control of an 18-wheeler, killing a National Guardsman by the name of Terry Frye.

In Ontario, California, a semitruck driven by an undocumented immigrant crashed on Interstate 10, killing three Americans and injuring several others. In St. Lucie County, Florida, a commercial truck driver with limited English proficiency made an illegal maneuver on the Florida Turnpike, and it resulted in a crash and killed three people. In Washington State, an undocumented commercial driver struck a stopped vehicle on a State highway killing a motorist.

These are not just statistics. These are families. These are brothers and sisters, mothers and fathers, daughters and sons, people whose families were destroyed because of what happened. Once again, it does come back to control.

When States abandon enforcement of Federal law, Americans—American families—suffer the consequences. Safety on American roads is not optional. American roads should be controlled by Americans. American data should be controlled and protected by Americans and American safety standards should be enforced for the benefit of Americans.

I thank the witnesses for being here today, and I do look forward to your testimony.

I now recognize the Ranking Member from the great State of Texas, Ms. Crockett, for an opening statement.

Ms. CROCKETT. Thank you so much, Mr. Chair. Thank you to the witnesses for appearing today to discuss threats to our transportation system.

This is a serious national security issue. I appreciate the opportunity to have a bipartisan discussion, something that does not happen very often here, about how our foreign adversaries target America's critical infrastructure.

Just last fall, the Federal Highway Administration warned that spyware had been found inside foreign-manufactured systems used to operate the signs, traffic cameras, weather stations, and vehicle chargers that line our highways all across the country. These communication devices could be used to collect individuals' transportation data, could be used to hack into government systems, and could even be used to cause outages in major American cities.

Infiltration of our supply chains is just one vulnerability our adversaries can exploit. We consistently see our adversaries target our critical infrastructure with cyber espionage and cyberattacks.

Unfortunately, from sending the names of CIA operatives over email to including a journalist in a Signal group chat discussing war plans, President Trump's Administration has shown a blatant disregard for our cybersecurity. The President has gutted the Cybersecurity and Infrastructure Security Agency, our core civilian cyber defense agency. He also fired the head of the U.S. Cyber Command, DHS' Cyber Safety Review Board, and cybersecurity professionals at the NSA and NIST.

The DHS determined the Critical Infrastructure Partner Advisory Council as a key advisory group that provided space for public-private collaboration to coordinate and craft cybersecurity plans to protect critical infrastructure. Experts repeatedly emphasize that public-private partnerships are necessary to protect the cybersecurity of our critical infrastructure. The Cybersecurity Information Sharing Act, which facilitates the public-private cyber threat intelligence ecosystem, expired last fall, and the Republican-led Congress has failed to reauthorize it.

President Trump's Administration has also disbanded key operations targeting foreign malign influence. Attorney General Pam Bondi dissolved the FBI's Foreign Influence Task Force. Director of National Intelligence Tulsi Gabbard dismantled the intelligence community's Foreign Malign Influence Center.

It appears that there is no longer any Federal body dedicated to tracking and analyzing foreign-State efforts to interfere in American society. Meanwhile, the President seems to get friendlier with the heads of authoritarian adversarial Nations every day.

This dismantling of the Federal Government's cybersecurity and national security resources and the continued politicization of our Federal agencies has left State and private officials reluctant to trust and share information with our Federal Government. This threatens the security of all critical infrastructure, from our healthcare to our elections to our transportation systems.

It is vital that we address the ways our foreign adversaries target our key critical infrastructure sectors. In my opinion, the largest threat to our national security and critical infrastructure is not undocumented immigration or foreign investment. It is the incompetent folks at the highest levels of our government that have dismantled our cybersecurity resources.

Thank you, and I yield back.

Mr. VAN DREW. I thank the Ranking Member. With that, I will recognize the Ranking Member of the Full Committee, Mr. Raskin.

Mr. RASKIN. Thank you very much, Chair Van Drew. Thank you to all our witnesses for joining us today.

To the extent that our colleagues have called this hearing to examine how foreign threat actors are compromising our national security by targeting transportation and critical infrastructure, that is a valid and meaningful subject of inquiry. I salute the Chair for this initiative.

China is in strategic competition with the United States and is using cyber espionage to undermine our defenses. Cybersecurity is of serious concern in the transportation sector because of the vast number of targets that operate new technologies and are run by a wide array of government and private entities.

From AI-driven software to trip-reliant hardware, advancement in technology of course has great promise to make transportation faster, cheaper, and safer. We must be vigilant to ensure these systems are not vulnerable to infiltration or attack from malign actors, like Putin's autocratic Russia or the Stalinist bureaucrats of China.

We cannot honestly discuss and debate the issue without addressing how President Trump has gutted the safeguards that protect our transportation and critical infrastructure against foreign threats. The programs and personnel in the U.S. Government that

keep us safe have been cut wholesale and have been bizarrely politicized, jeopardizing our national security.

Trump removed a third of the workforce at the Cybersecurity and Infrastructure Security Agency, which helps government and business work together to identify cyber threats before it is too late. That reduction included the Department officials dedicated to local government coordination with business, which is crucial to transportation infrastructure security.

Trump fired the Chair of the Joint Chiefs and other top-level military leadership, eliminating continuity in national security, and his Attorney General shut down the FBI's Foreign Influence Task Force, the group responsible for identifying and combating malign foreign influence operations targeting the people of the United States.

Trump's approach to national security, especially cybersecurity, is that of a coach who is friendly with the coaches of foreign teams and then suddenly takes his goalie off-net. To my mind, I don't think we can have a serious conversation about hardware vulnerabilities if we are going to ignore the fact that President Trump has made our infrastructure substantially less safe in just one year's time.

What is even more confusing to me about today's hearing is that we are examining foreign threats as though Donald Trump isn't systematically ceding more global power to China every single day, even as he multiplies and deepens his own personal business ties to China.

During his first term, Trump collected millions of dollars in payments from the Chinese Government and State-owned companies. In exchange for these unconstitutional emoluments, he opposed sanctions against Chinese telecom companies and banks even when they threatened our national security. He even tried to cancel military exercises with Japan and South Korea because China complained about them.

In his second term, we have seen even more of enthusiastic Presidential embrace of the tyrants and dictators. Over the last year, the administration has dismantled USAID, giving China free rein to swoop in and offer countries around the world assistance with their infrastructure construction projects, their agricultural programs, their food aid, and public health, dramatically expanding China's sphere of influence.

Trump has also hurt American consumers by imposing unlawful and arbitrary tariffs and hamstrung our ability to respond to threats by firing government workers, including key experts on China and national security personnel. All the while, he has been using his crypto ventures to pocket hundreds of millions of dollars directly from Chinese billionaires with ties to the CCP.

In May, a tiny Chinese tech company with ties to the government announced it had bought \$300 million of President Trump's memecoin, despite the fact that it has no revenue and only eight employees. Gee, I wonder where the money is really coming from.

One year in Trump's second term, we've learned that other countries think that Donald Trump is indeed making a country great, but that country is not America. It is China. In a 21-country poll by the European Council on Foreign Relations, the majority of re-

spondents around Europe said that while the U.S. is less feared by its adversaries and less revered by its friends, they fully expect China's global influence to continue to grow over the next decade.

It is no wonder why they think, Mr. Chair, when Trump is inviting China, an egregious human rights violator, to join the Gaza Board of Peace and reverse its course and allows U.S. chip exports to China in a move that Anthropic CEO likened to selling nuclear weapons to North Korea.

My friends, I wish this could just be about the problem of hardware technology in transportation, but it exists in this larger political context. That we have to make that clear for everyone if we are serious about confronting the problem of Chinese and Russian tyrannical influence in our government.

Thank you, Mr. Chair. I yield back.

Mr. VAN DREW. I thank the Ranking Member.

Let me say—only conjecture here. I am not sure, but I have this sneaking suspicion, this intuitive feeling, the other side doesn't like President Trump all that much. Am I right?

Ms. CROCKETT. I have never met him.

Mr. RASKIN. I have never met him. It is not personal. We were looking just at what the effect is on the American people.

Mr. VAN DREW. I know. I am trying to have a little levity.

With that, I thank Mr. Raskin. Without objection, all other opening statements will be included in the record.

Mr. VAN DREW. We will now introduce today's witnesses. The first witness—I am going to try not to murder your name; we will see how I do—Ms. Emily de La Bruyère. Pretty close? OK. Thank you for being here. The floor is yours.

Ms. DE LA BRUYÈRE. Thank you. Thank you, Chair Van Drew—

Mr. VAN DREW. Actually, let me—you know what? Let me do a little history of you. I am sorry. You are a Senior Fellow at the Foundation for Defense of Democracy. It is a think tank that conducts research on our national security and foreign policy issues. Your work focuses on China, economic security, international organizations, and supply chains.

Now the floor is yours.

STATEMENT OF EMILY DE LA BRUYÈRE

Ms. DE LA BRUYÈRE. Thank you, Chair Van Drew. Thank you, Ranking Member Crockett. Thank you for this opportunity and both having names much easier to pronounce than mine.

The Chinese Communist Party wants to control global resources, markets, and information so that it can control the world. Beijing pursues this ambition by leveraging nonmarket industrial policy through which it subverts critical supply chains and networks, a strategy of military-civil fusion through which it turns that positioning into a forward-deployed military presence, and a program State-sponsored data collection through which every Chinese company and component becomes an asset for influence and espionage.

Transportation systems are a core part of this Chinese strategy. Beijing defines transportation systems as part of the military-civil fusion ecosystem because they are necessary for industrial operations, social functioning, and military mobilization. For that rea-

son, China protects its own transportation systems domestically while looking to penetrate them internationally.

Transport systems also represent a massive economic opportunity. The U.S. auto sector, for example, alone accounts for some 11 million jobs and \$1.2 trillion of national output a year. Beijing wants those markets. Beijing also wants the military-relevant tech and industrial capacity that undergirds them.

China wants something else from transportation systems, too. Today's technological trends are pushing the transport ecosystem toward an intelligent, connected, data-is-everything paradigm. In that environment, every foothold in a transport system, whether that is a component or a piece of software or a vehicle, becomes a possible back door. Everything is a computer. China is hacking all of it.

For this reason, China's presence in U.S. transportation systems, (a) threatens U.S. industry and supply chains and markets, and (b) grants Beijing access to critical information on American society, the power to influence that information and therefore society, and the ability to disrupt the foundational networks on which our country depends.

This isn't a notional danger. It is not something that is on the horizon. Our system is already embedded with Chinese components, and we are already under attack. LiDAR offers a valuable example. Autonomous vehicles use LiDAR to map their surroundings. Airports use it to track movement and crowds. Bridges use it to scan for defects.

China controls 90 percent of the world's LiDAR market. The Chinese entities that are leading this charge are companies like Hesai, RoboSense, DJI that the U.S. Government has already identified as tied to the Chinese military. Those Chinese military-tied companies sell to GM's Cruise and Nvidia's Drive Hyperion. Their LiDAR sensors have been installed at JFK International Airport and Charlotte Douglas International Airport.

Chinese LiDAR sensors are on intersections in Chattanooga and on drawbridges in Sarasota. Every purchase of a Chinese LiDAR sensor funds the Chinese Communist Party. Every Chinese LiDAR sensor risk collecting information on behalf of Beijing, and all of them could be turned off at China's command.

This isn't a unique case. LiDAR is not isolated. The same story plays out across the broader ecosystem of components that go into modern transportation systems, whether those are IoT modules, optical transceivers, or cameras.

Moreover, moving beyond the component level, Beijing is also building out the platform and software level of modern transportation. China is the world's largest player in in-car AI agents. Beijing is also developing unrivaled global shipping and transportation and logistics solutions, for example, LOGINK, a Chinese national platform that provides a centralized window into the otherwise fragmented world of global shipping under the Chinese Government's control.

Washington needs to stop further Chinese penetration of our transportation systems. Those efforts can start with direct restrictions. No company that uses Chinese components software or those made by a Chinese-influenced entity should be eligible for Federal

procurement, Federal tax incentives, or any other Federal incentives. In establishing restrictions like that, Washington should also tighten and clarify FEOC and PFE rules to make it clear what it is that is a Chinese entity and to make that a stricter definition.

Targeted measures like this can directly bolster the security of American transportation systems, but Washington should also take broader action to change the State of play that has allowed China to embed itself into our critical infrastructure systems. Tariffs on Chinese goods can help dissuade the U.S. private sector from buying from Chinese entities and therefore from being complicit with the Chinese Communist Party. Tariffs can also create the circumstances in which to rebuild a trusted American industry.

On the data front, no company that stores data in China should be permitted to collect data in the United States or be eligible for Federal procurement, defense industrial-based procurement, Federal tax credits, or other incentives. Washington should leverage trade deals to compel U.S. allies and partners to enact their own defenses against China, such that they don't serve as conduits for the Chinese Communist Party.

It might seem impossible now to think that China could supplant American giants like FedEx, Boeing, and Ford. That scenario is on the very, very near horizon. Should it come to pass, China will claim a determinative advantage. Washington needs to fight back.

Thank you for your time.

[The prepared statement of Ms. de La Bruyère follows:]

TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Judiciary Committee

Embedded Threats: Foreign Ownership, Hidden Hardware, and Licensing Failures in America's Transportation Systems

EMILY DE LA BRUYÈRE

Senior Fellow
Foundation for Defense of Democracies

Washington, DC
January 21, 2026



www.fdd.org

Chair Van Drew, Ranking Member Crockett, thank you for the opportunity to testify today.

The Chinese Communist Party (CCP) wants to control global resources, markets, and data — so that it can control global prosperity, security, and information. Beijing pursues this ambition by leveraging non-market industrial policy through which it subverts critical supply chains and networks; a strategy of “military-civil fusion” through which it converts that civilian positioning into a forward-deployed military presence; and a state-sponsored program of data collection and aggregation through which every Chinese company, component, and platform becomes positioned for espionage and influence.

Transportation systems are a core part of this Chinese strategy. Transportation systems encompass vehicles themselves, whether rail cars or autonomous cars; the infrastructure on and through which they operate, such as toll systems and bridges; and the components and platforms that power them, ranging from in-car artificial intelligence (AI) agents to semiconductors to LiDar.

China’s Framing and Threat

Transportation systems fall within Beijing’s framing of the “military-civil fusion” ecosystem. They enable social functioning, industrial operation, and military mobilization. China therefore both protects them domestically and seeks to penetrate them internationally.¹

Transportation systems also represent a massive economic opportunity. These are industries of industries. Their markets are enormous. So are those of the industries they drive, like rubber for tires, sensors for toll systems, and aluminum for capacitors. Across the board, the relevant industrial and technological capacity has direct military applications; it generates security as well as economic rewards. Beijing therefore wants to capture global transportation markets, supply chains, and industrial and technological capacity. And Beijing wants to do so at the expense of its rivals, namely the United States.

Modern technological trends both generate a unique opportunity for Beijing to succeed and raise the stakes of such success. The intelligent, connected era is revolutionizing transportation. This creates an opening for a disruptor — China — to upset incumbents in the sector, the United States and the West. Beijing is rapidly securing dominance over emergent inputs into modern transportation systems. These include components like semiconductors and sensors, software and transportation platforms, and vehicles themselves, whether smart cars or electric buses. In many cases Beijing is doing so without broad recognition of its menace — because of its incremental

¹ See, for example, the “军民融合发展战略纲要 [Outline of the Strategy for Integrated Military and Civilian Development],” issued by the Central Commission for Integrated Military and Civilian Development in 2018; Annie Fixler, RADM (Ret.) Mark Montgomery, and Rory Lane, “CSC 2.0: Military Mobility Depends on Secure Critical Infrastructure,” *Foundation for Defense of Democracies*, March 27, 2025. (<https://cybersolarium.org/csc-2-0-reports/military-mobility-depends-on-secure-critical-infrastructure>)

approach and because, capitalizing on a new technological paradigm, Beijing is playing a different game than incumbents in the sector.

Perhaps most importantly, today's technological revolution means that every foothold in the transportation sector — every component, software system, and vehicle — is a strategic as well as an economic asset; a possible back door to collect, disrupt, and shape information. Everything is a computer. China is hacking all of it.

China's efforts to co-opt U.S. and global transportation systems, therefore, do not only create supply chain and market risks, threatening the autonomy and economic rewards that come from industrial capacity. China's subversion also grants Beijing access to critical information on American society; the ability to influence that information; and the power to destabilize foundational systems on which American society depends.

The State of Play

This is not a notional danger. China's presence is already well advanced. The United States is already under attack.

Take, for instance, LiDar.² LiDar is used by autonomous vehicles to map their surroundings, by airports to track movement and crowds, by toll systems to detect vehicles, and by road and bridge operators to scan for defects. Thanks to non-market support, including subsidies and backing from the military-civil fusion apparatus, Chinese companies dominate the sector: They claim more than 93 percent of the global automotive LiDar market and almost 90 percent of the total LiDar market.³

Among China's leading LiDar champions are companies — like Hesai Technology, Huawei, and DJI — that the U.S. government has identified as Chinese military companies. The Pentagon recently concluded that another top Chinese LiDar company, Robosense, also merits inclusion on the Pentagon's 1260H list of military-linked Chinese companies.⁴ Hesai supplies Amazon's Zoox, Aurora Innovation, General Motors's Cruise, and Nvidia's Drive Hyperion.⁵ Hesai's LiDar sensors are used at the Charlotte Douglas International Airport and Portland International Airport — and have been installed at intersections in Chattanooga, Tennessee, and on drawbridges in Sarasota, Florida. LiDar sensors from DJI's LiDar subsidiary Livox have been deployed in major

² LiDar is a remote sensing technology that uses pulsed laser light to measure distances.

³ "China takes the lead in automotive LiDAR: A market set to quadruple by 2030," *Yole Group*, June 24, 2025. (<https://www.yolegroup.com/press-release/china-takes-the-lead-in-automotive-lidar-a-market-set-to-quadruple-by-2030>)

⁴ "Pentagon seeks to add Alibaba, Baidu, BYD to China military list, Bloomberg News reports," *Reuters*, November 26, 2025. (<https://www.reuters.com/world/china/pentagon-suggests-adding-alibaba-baidu-byd-list-aiding-china-military-bloomberg-2025-11-26>)

⁵ Daniel Ren, "Nvidia chooses China's Hesai for lidar sensors in Hyperion autonomous driving platform," *South China Morning Post*, January 6, 2026. (<https://www.scmp.com/business/china-business/article/3338909/nvidia-chooses-chinas-hesai-lidar-sensors-hyperion-autonomous-driving-platform>)

American transit hubs ranging from Moynihan Hall/Penn Station to JFK International Airport.⁶ RoboSense supplies Lucid Motors and Rivian. Dallas Fort Worth International Airport in 2025 announced that it would procure Robosense LiDar.⁷

Every purchase of a Chinese LiDar sensor funds the Chinese Communist Party. Every Chinese LiDar sensor — whether in electronic tolling systems, autonomous vehicles, or airports — risks collecting information for Beijing. And all could be turned off at China's command.⁸

A similar story holds across the larger ecosystem of components that power intelligent transportation. Internet of Things (IoT) modules enable fleet management and IoT-based tolling. China is the world's largest player in that market — thanks to companies that the U.S. government has identified as Chinese military companies like Quectel and China Mobile.⁹ Optical transceivers support traffic signal control networks; railway, highway, and airport communication systems; and in-vehicle communication among cameras, radar, LiDar, and ultrasonic sensors.¹⁰ China's Innolight alone holds more than 10 percent of the global market for optical transceivers.¹¹ Also in the list of top companies are China's Accelink, China's Huawei Hisilicon, and China's Eptolink.

Like LiDar, these components collect data, are vulnerable to attack, and are essential inputs into not only transportation systems but also data, communication, and computing infrastructure. As with LiDar, Beijing is deliberately securing a stranglehold over their global markets. And as with LiDar, the U.S. transportation ecosystem is embedded with them.

Increasingly, Beijing is also developing the platform level for modern transportation systems. This includes in-car software systems, ranging from legacy navigation software, like AutoNavi, to emergent, AI in-car agents like Simo, developed by a joint venture between Geely and Baidu. China's platform positioning also includes global smart shipping and supply chain networks like Alibaba's Cainiao and logistics solutions like China's National Transportation Logistics Platform

⁶ “Comments on ‘Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles’ Proposed Rule,” *Coalition for Safe and Secure Technology*, April 30, 2024.

(<https://secureenergy.org/safes-coalition-for-reimagined-mobilitys-comments-on-the-department-of-commerces-securing-the-information-and-communications-technology-and-services-supply-chain-connected-vehicles-notice>)

⁷ Anne-Sophie Dubois, “Dallas Fort Worth Airport Selects Outsight for the World's Largest 3D LiDAR Deployment,” *Outsight*, December 15, 2025. (<https://insights.outsight.ai/dallas-fort-worth-airport-selects-outsight>)

⁸ RADM (Ret.) Mark Montgomery, “Lidar: Another emerging technology brought to you by China,” *Defense News*, April 25, 2024. (<https://www.defensenews.com/opinion/2024/04/25/lidar-another-emerging-technology-brought-to-you-by-china>); Craig Singleton and RADM (ret.) Mark Montgomery, “Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems,” *Foundation for the Defense of Democracies*, December 2, 2024. (<https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems>)

⁹ Charles Parton, “Chinese cellular (IoT) modules: Countering the threat,” *Council on Geostrategy*, March 19, 2024. (<https://www.geostrategy.org.uk/research/chinese-cellular-iot-modules-countering-the-threat>)

¹⁰ Optical transceivers are interconnected components that can transmit and receive data.

¹¹ “Top Optical Transceiver Manufacturers List (2024),” *Optcore*, June 26, 2024. (<https://www.optcore.net/article056/?srsltid=AfmBOoqZqoVdbqUd58RmiFSrAhgIPBuBCAeGGsbIPDyNFFQPWSyM4BZQ>)

(LOGINK). LOGINK provides a centralized window into the otherwise fragmented world of global shipping, under the Chinese government's control.¹² Like China's component-level footholds in transportation systems, these platforms grant the Chinese Communist Party access to information and the ability to disrupt international movement. These platforms also empower Beijing to *shape* that information, the movement it defines, and the markets built on top of it.

China's presence, at a component and a platform level, in American transportation systems grants Beijing the power to turn off U.S. infrastructure. But even short of such an attack, China's footholds, already and constantly, allow the Chinese Communist Party to collect data on Americans that threatens citizens' privacy and the country's competitiveness. As I speak, Beijing is monitoring which Americans are moving where. In doing so, Beijing collects large-scale data on American society. That data amounts to a strategic asset.

China's presence in transportation systems also attacks the U.S. industrial base. Beijing uses its footholds in supply chains to move up the value chain — from, for example, car parts to car modules to car software to cars themselves. Beijing accomplishes this through non-market and illicit means, like forced tech transfer and intellectual property theft. Beijing also does so through entirely licit avenues, like the collaboration of U.S. and international champions desperate for access to China's market, production, and expertise.

As China moves up the value chain, its threat to transportation systems, and therefore to America, becomes both more firmly embedded and larger. The information that a single software system in a car collects pales next to that gathered by the car as a whole.¹³ The consequences of a LiDAR sensor being deactivated pale next to those of entire fleets of vehicles being turned off.

In addition, the growing sophistication of China's industrial offensive in the transportation sector attacks the heart of U.S. industry — including the defense industrial base. If China subverts the global auto industry, America will lose some 11 million jobs and 1.2 trillion dollars in output.¹⁴ If China subverts the aviation industry, the U.S. will lose some 1 million jobs and \$250 billion in output.¹⁵ Those figures represent our sovereign industrial base. Losing those jobs and dollars will mean losing the industrial and technological capacity needed to sustain America's military and innovate for our security.

¹² "China's National Transportation Logistics Project," *Horizon Advisory*, August 2021.

(<https://www.horizonadvisory.org/geopolitical-operating-system>)

¹³ Elaine K. Dezenski, "Trojan Horse: China's Auto Threat to America," Testimony before the House Select Committee on Strategic Competition Between the United States and the Chinese Communist Party, December 11, 2025. (<https://www.fdd.org/wp-content/uploads/2025/12/Elaine-Dezenski-Testimony-12.11.25.pdf>)

¹⁴ "Alliance for Automotive Innovation Releases NEW Economic Data," *Alliance for Automotive Innovation*, January 29, 2025. (<https://www.autosinnovate.org/posts/press-release/auto-innovators-data-driven-report-release>)

¹⁵ Brianna Wilson, "Understanding the Leadership Position of U.S. Aviation Manufacturing," *Monitor Daily*, February 4, 2025. (<https://www.monitordaily.com/understanding-the-leadership-position-of-u-s-aviation-manufacturing>)

This is a near threat. Thanks to its dominance at the upstream of the supply chain, its dedicated industrial and technology strategy, and the willingness of U.S. and international champions to hand over research and development, China's auto champions are increasingly the world's. BYD — one of China's most heavily subsidized companies — overtook Tesla in 2025 to become the world's largest EV seller. The average price of a BYD vehicle is about \$17,000, compared to about \$40,000 for a new Tesla. The same story risks playing out in the aviation industry. In no small part due to its partnerships with Airbus, China's state-owned COMAC is directly challenging that company and Boeing with its C919.¹⁶

What To Do: A Path Forward

China's ambitions in the transportation sector, and the corresponding danger to the United States, are not new. They date back more than a decade. But the situation is newly urgent. The sector is at a tipping point. Without action, America will sacrifice security, prosperity, and freedom.

But action is possible.

The first step is to stop further Chinese penetration of transportation systems; to protect critical U.S. infrastructure from Huawei and hidden Huaweis. Washington should prohibit any transportation system or company that incorporates components or software made by Chinese or Chinese-influenced companies from receiving federal dollars, tax credits, or other incentives.

In the process, Washington should tighten the definition of what it means to be a Chinese or Chinese-influenced company. That definition should build on the U.S. Commerce Department's framing of a "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary." The definition should cover any company that is owned or invested in by Chinese entities; is under Chinese jurisdiction; has a tech licensing deal with a Chinese entity; localizes data, research, development, or production in China; or that invests in Chinese entities. This ban and definition should be both strictly framed and strictly enforced to protect against Chinese circumvention, localization, and other means of evasion. Prohibited Foreign Entity (PFE) and Foreign Entity of Concern (FEOC) rules provide an immediate opportunity to implement and scale such restrictions across sectors, including transportation.

These targeted measures can catalyze immediate change in and send a signal about China's presence in American transportation systems. But Washington must also take broader action to change the fundamental state of play that has allowed Beijing to secure its current footholds across America's critical infrastructure.

That action starts with protecting the U.S. market from China. Higher tariffs on Chinese goods can help to neutralize the non-market industrial offensive through which Beijing distorts markets

¹⁶ Stuart Lau, "EU Champion Airbus has deep links to Chinese military industrial complex, report says," *Politico*, June 22, 2022. (<https://www.politico.eu/article/eu-champion-airbus-has-deep-links-to-chinese-military-industrial-complex-report-says>)

and co-opts supply chains. Such tariffs can dissuade the U.S. private sector from purchasing Chinese products and thereby becoming complicit with Beijing's industrial offensive. Tariffs also provide the conditions necessary to rebuild the domestic industry that the CCP has decimated.

In parallel, Washington can also protect American data — with it, the privacy of Americans and the country's competitiveness. No company that stores data in China should be permitted to collect data in the United States, or be eligible for federal procurement, federal tax credits or other incentives, or defense-industrial base procurement.

Washington must activate the U.S. private sector. Extant business models effectively hinge on forfeiting valuable U.S. technologies and positioning to China — and reject proactive investments in domestic industry. Washington can change that. The American private sector should have to choose between the U.S. and Chinese markets. Washington should prohibit any Chinese company, as well as any company that leverages components from, has a tech licensing deal with, has investment from, or has a joint venture with a Chinese company, from defense-industrial base procurement, federal procurement, or federal tax credits.

The U.S. must also recognize that the U.S.-China competition is not a bilateral one. China's presence is global. Defending against it requires a global approach. Washington should leverage trade deals, including a reauthorized USMCA, to compel American allies and partners, and American allied and partner private sectors, to implement their own protections against China, rather than serving as conduits for the Chinese Communist Party to establish overseas beachheads and access to the United States.

All of these measures are sticks. There are carrots for Washington to offer, too. Removing China from the American market broadly, and the transportation sector specifically, will incur short-term costs. It is up to Washington to ensure that, after decades of decimation at Beijing's hands, U.S. industry has the conditions necessary to succeed; and that investment, commercialization, and production in the United States are possible and potentially profitable. Washington should provide the infrastructure necessary for production, including through the expanded provision of domestic and upstream resources, a permissive regulatory environment, and a skilled workforce. And Washington should provide incentives for trusted companies and solutions to replace China's in American transportation infrastructure.

America has a chance to reindustrialize and renew — and, in the process, to restore national security. The transportation sector should be core to that effort. It might seem impossible now to think that China could supplant American giants like Ford, Boeing, and FedEx. But that scenario is on the horizon. And the industrial and technological capacity, supply chain leverage, data advantage, and coercive power that Beijing is positioned to capture through its transportation subversion will help the Chinese Communist Party win out more broadly. Washington must fight back.

Mr. VAN DREW. Thank you. Very informative. That outlines the seriousness of this issue. I know it is not the sexiest issue in Congress that everybody is talking about, and I get it. This room should be packed, and everybody should hear this and listen to it. It is a serious, serious issue.

Again, as I said before—and I understand components of what you are talking about in your issues, but it should be a bipartisan one as well.

Now, your name, on the other hand, Mr. Cole, is Rocky Cole. Couldn't be easier than that, right?

Mr. COLE. Correct.

Mr. VAN DREW. The floor is yours.

STATEMENT OF ROCKY COLE

Mr. COLE. Thank you, Chair Van Drew, Ranking Member Crockett, and the distinguished Members of the Committee, for the opportunity to testify today.

The topic of the hearing is embedded threats in America's transportation systems, and I will certainly address those directly. However, I believe, as several other people have pointed out, that these threats are best understood in the broader context of adversarial cyber operations against America's critical infrastructure as they constitute one piece of a larger strategic landscape.

My name is Rocky, and I have worked to counter America's top cyber adversaries for almost 20 years now, first within the United States intelligence community, then at Google, and now at a U.S.-based, venture capital-backed company called iVerify, which secures the very powerful computers in our pockets, mobile phones.

I have witnessed a strategic evolution of cyber operations from the earliest days of mere cyber espionage to what can only be called today's cyber cold war. My experiences have informed a somewhat unique perspective on both the problem and steps we can take to mitigate the threats.

In cyberspace, America has two historical rivals, China and Russia. Historically, both Chinese and Russian cyber operations were focused on intelligence gathering. For China, this meant extracting intellectual property to feed their Made in China 2025 strategy, which a former Director of the NSA described as the greatest transfer of wealth in human history, while Russia focused on more traditional espionage goals.

However, we have recently, in within the last five years, reached a watershed moment where the objective of cyber operations has shifted to prepositioning for disruptive effects. Modern doctrine now views cyberspace as a basic platform for hybrid warfare where blinding cyberattacks are intended to paralyze command-and-control networks before kinetic operations even begin.

The U.S. intelligence community assesses with high confidence that these actors are embedding, quote, "sleeper software" within our infrastructure to be activated at will. The threat from China is particularly acute through several multiyear campaigns aimed at achieving information dominance. The Volt Typhoon campaign, for example, targets energy, water, and yes, transportation sectors specifically to disable military mobilization and sow domestic chaos

that would distract U.S. leaders during the potential invasion of Taiwan.

Furthermore, Salt Typhoon has compromised the backdoor systems used by telecommunication providers for court-ordered wiretapping and allowing China to monitor law enforcement, track the real-time geolocations of millions of Americans, and compromise our mobile devices. These operations have even expanded to targeting toll systems and compromising State-level commercial driver's license databases, all which are vital for our national logistics.

To evade detection, these actors have refined their methods to bypass modern defenses through malware-free intrusions. They utilize techniques like living off the land, which means using legitimate system administration tools to blend in with normal activity and avoid detection, using largely stolen credentials like passwords and tokens as their initial access point.

Finally, as per the topic of this hearing, they increasingly utilize supply chain operations to gain backdoor access to critical technologies. This could manifest as tampering with or implanting hardware components, inserting malicious codes into software updates, or compromising the integrity of manufacturing processes for devices like routers, servers, and even large industrial equipment such as port cranes.

Despite the magnitude of the threat, the United States remains hamstrung by a patchwork regulatory landscape and structural challenges that impede a unified defense. Our defensive posture is characterized by voluntary frameworks that have failed to keep pace with the adversary's strategic pivot to prepositioning. Compounding this is the complexity of coordinating between the Federal Government and 50 State-level regulatory bodies.

This asymmetry demands a significant structural and legal overhaul to achieve true cyber deterrence both on the offensive side and on the defensive side. This includes formalizing the authority for the United States Cyber Command to, quote, "defend forward and disrupt adversarial groups within foreign networks before they reach the homeland."

We must also address systematic personnel failures within the United States Cyber Command by transitioning toward an independent cyber force that establishes uniform standards for recruitment and training and bypasses the traditional military standards that have frankly hindered our cyber readiness. Most importantly, we should consider advancing a framework that treats cyberattacks on critical infrastructure that may imperil a human life as the acts of war that they are, equivalent to kinetic strikes.

We must also harden our domestic resilience by moving beyond purely voluntary standards. Congress should fund States to build high-maturity response capabilities and convert voluntary resilience standards into mandates for systematically important entities requiring redundant power and physical hardening across physical sectors. We must shift the legal duty of care to software manufacturers and away from the end users like local governments, instead holding the software designers liable for design flaws while mandating a move to secure-by-design principles rather than today's voluntary pledges.

Finally, to mitigate supply chain risks, Congress should consider implementing mandatory screening and the eventual phase-out of Chinese-manufactured hardware with remote communications capabilities within highly sensitive critical infrastructure and Federal networks, akin to the rip-and-replace campaigns that Congress has already funded to remove Chinese-made telecommunications gear from America's core networks.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Cole follows:]

Testimony of
Rocky Cole
Co-Founder & COO of iVerify

Before

House of Representatives
Committee on the Judiciary
Subcommittee on Oversight

"Embedded Threats: Foreign Ownership, Hidden Hardware, and Licensing Failures in America's Transportation Systems"

January 21, 2026

Chairman Van Drew, Ranking Member Crockett, and distinguished members of the Committee, thank you for the opportunity to testify on threats to America's critical infrastructure, many of which are hiding in plain sight.

I've worked to counter America's top cyber adversaries for almost twenty years now, first within the United States Intelligence Community, then at Google, and now at a U.S.-based, venture-capital backed company called iVerify, which focuses on securing the highly sophisticated computers we all keep in our pockets, mobile devices. I've witnessed the strategic evolution of cyber operations, from the early days of cyber espionage to today's Cyber Cold War, and my experiences have informed a unique perspective on both the problem and steps we can take to mitigate these threats.

The topic of this hearing is embedded threats in America's transportation systems, and I plan to address those directly; however, these threats are best understood in the broader context of America's critical infrastructure, as they constitute one piece of a larger strategic landscape.

Historically, both Chinese and Russian cyber operations were focused on intelligence gathering. For the PRC, this meant extracting intellectual property to feed their "Made in China 2025" strategy, while Russia focused on political interference. However, we have reached a watershed moment where the objective has shifted to pre-positioning for disruptive effects. Modern doctrine now views cyberspace as a basic platform for hybrid warfare, where blinding cyberattacks are intended to paralyze command and control networks before kinetic operations even begin. U.S. intelligence assesses with high confidence that these actors are embedding "sleeper software" within our infrastructure to be activated at will.

Today, the United States faces a sophisticated doctrine of strategic pre-positioning within our critical infrastructure by our key adversaries. This evolution represents a transition from opportunistic data theft and political espionage to the systematic infiltration of the systems that underpin modern life—including our telecommunications, energy, water, and yes, transportation

networks. By embedding themselves in these sectors, these actors have created a persistent threat designed to support kinetic military operations during future crises.

The threat from China is particularly acute through several multi-year campaigns aimed at achieving "information dominance." The Volt Typhoon campaign targets energy, water, and transportation sectors specifically to disable military mobilization and to sow domestic chaos that would distract U.S. leaders during a potential invasion of Taiwan. Furthermore, Salt Typhoon has compromised the "backdoor" systems used by telecommunications providers for court-ordered wiretapping, allowing the PRC to monitor law enforcement, track the real-time geolocation of millions of Americans, and compromise mobile phones. Their operations have even expanded to targeting toll systems through SMS phishing and compromising state-level commercial driver's license databases, which are vital for our national logistics.

Simultaneously, Russia continues to integrate cyber operations directly into its military campaigns, using Ukraine as a testbed for destructive tactics. Their Sandworm unit, considered the apex of destructive state-sponsored hacking, has integrated "wiper" software designed to ruin industrial control systems in the energy and telecommunications sectors. Since 2022, they have also conducted sustained reconnaissance on air, sea, and rail transportation to disrupt the delivery of assistance to Ukraine. These state actors are further supported by affiliated hacktivists who perform opportunistic attacks on U.S. water and energy infrastructure by capitalizing on unsecured network connections.

To evade detection, these actors have refined their methods to bypass modern defenses through "malware-free" intrusions. They utilize "Living off the Land" techniques, using legitimate system administration tools to blend in with normal activity and avoid detection. They rapidly exploit high-severity vulnerabilities in firewalls and VPNs within days of disclosure and increasingly target less-monitored devices, like employee mobile phones, to steal credentials. Furthermore, they hijack domestic consumer infrastructure, such as end-of-life routers and internet-of-things devices, to create operational relay networks that mask the origin of their traffic.

And finally, as per the topic of this hearing, they increasingly utilize supply chain operations to gain backdoor access to critical technologies. This can manifest as tampering with or implanting hardware components, inserting malicious code into software updates, or compromising the integrity of manufacturing processes for devices like routers, servers, and even large industrial equipment such as port cranes.

Despite the magnitude of the threat, the United States remains hamstrung by a patchwork regulatory landscape and structural challenges that impede a unified defense. Our defensive posture is characterized by voluntary frameworks that have failed to keep pace with the adversary's strategic pivot to pre-positioning. Compounding this, the complexity of coordinating between federal and 50 state-level regulatory bodies creates systemic gaps that adversaries readily exploit. On the offensive side, limited authorities and an over-reliance on dated international norms have often restricted the efficacy of U.S. cyber operations, allowing adversaries to operate from sanctuaries with relative impunity.

This asymmetry demands a significant structural and legal overhaul to achieve true cyber deterrence.

This includes formalizing the authority to "Defend Forward" by disrupting adversarial groups within foreign networks before they reach the homeland. We must also address systemic personnel failures within the United States Cyber Command by transitioning toward an independent Cyber Force that establishes uniform standards for recruitment and training, bypassing traditional military standards that often hinder cyber readiness. Most importantly, we should consider advancing a framework that treats cyberattacks on critical infrastructure that imperil human life as acts of war equivalent to kinetic strikes.

We must also harden our domestic resilience by moving beyond voluntary standards. Congress should fund states to build high-maturity response capabilities and convert voluntary security goals into mandates for systemically important entities, requiring redundant power and physical hardening across all critical sectors. We must shift the legal "duty of care" to software manufacturers and away from end-users, holding them liable for design flaws while mandating a move to "Secure by Design" principals, rather than today's voluntary pledges. And finally, to mitigate supply chain risks, Congress must implement mandatory screening and eventual phase-out of Chinese-manufactured hardware with remote communications capabilities within highly sensitive critical infrastructure and federal networks, akin to the rip-and-replace campaigns Congress funded to remove Chinese-made telecommunications gear from America's core networks.

In conclusion, we must assume that our adversaries maintain persistent access to many of our critical systems. Reclaiming the operational advantage requires a unified strategy that fuses regulatory, industrial, and diplomatic efforts. While the U.S. moves toward "preemptive erosion" to hold adversaries' infrastructure at risk, we must simultaneously harden the home front through institutional reform and mandatory technical standards. Only through this combination of defending forward and securing the home can we hope to deter this latent threat from escalating into active, widespread disruption.

Thank you, and I look forward to your questions.

Mr. VAN DREW. Thank you, Mr. Cole. With that, let me say you're the co-founder and COO of iVerify, a cybersecurity company focused on mobile phones, and previously worked at Google and Deloitte and served with the National Security Agency.

Mr. Chris Spear is next. Mr. Spear is the President and Chief CEO officer of the American Trucking Association, an organization made up of trucking companies. He also serves on the Board of Directors for American Transportation Research Institute and the Trucking Cares Foundation.

Mr. Spear?

STATEMENT OF CHRIS SPEAR

Mr. SPEAR. Chair Van Drew, Ranking Member Crockett, and the Members of the Subcommittee, thank you for the opportunity to testify here today.

For over 90 years, the American Trucking Associations has represented an industry that employs the hardest-working men and women in the country. Safety is in our DNA, and it is at the forefront of everything that we do. The overwhelming majority of America's 3.6 million truck drivers take immense pride in their work. They meet every requirement every day, and they move our economy forward with proficiency and with pride.

Safely operating a tractor trailer requires specialized skills and an adherence to high standards of professionalism. A CDL should represent a promise that the person behind the wheel of an 80,000-pound vehicle is qualified, competent, and accountable.

Regrettably, years of lax and uneven enforcement have undermined that promise. Serious vulnerabilities, particularly related to driver training and CDL issuance, have been exposed through several high-profile, tragic, and preventable crashes. CDL mills which masquerade as legitimate schools have fast-tracked prepared individuals into trucking by putting profits before training.

Meanwhile, State licensing agencies handed out improper credentials, and Federal regulators looked the other way, enabling unqualified individuals to climb into the driver's seat. ATA has long warned that insufficient compliance allows unsafe operators to obtain CDLs.

Fortunately, Secretary Duffy has made it a priority to close these loopholes. Our federation has been working hand-in-glove with USDOT to implement comprehensive solutions. We know that meaningful oversight works. Since December, FMCSA at DOT has removed nearly 7,000 CDL mills from the training provider registry and put an additional 450 noncompliant providers on notice.

These actions, coupled with upholding Federal driver qualifications and implementing regular audits, are critical steps toward improving the CDL system. We appreciate the Subcommittee's focus on these issues, and we look forward to being a resource as you seek to codify these regulations.

While the integrity of CDLs is foundational to highway safety, the systems that monitor driver compliance and enable roadside enforcement are just as critical. In recent years, the proliferation of noncompliant electronic logging devices has emerged as a serious and rapidly evolving threat. Cheating has gone high-tech, with

some devices using AI to produce fake documentation, like fuel and food receipts, to fabricate hours of service.

Equally concerning are digital back doors that could provide U.S. adversaries access to sensitive supply chain data. When operators are able to purchase devices that falsify logs or conceal violations, it rewards unsafe behavior and penalizes carriers who invest in compliant systems.

ATA strongly supports FMCSA's efforts to strengthen electronic logging device certification, which have led to the removal of nearly 100 noncompliant devices in just the last two months. An additional 250 devices have been removed, underscoring the need for better vetting on the front end. We urge Congress to improve device screening, apply greater scrutiny to foreign-owned ELDs, and enhance penalties against violators.

Another growing concern involves cross-border trade with Mexico. The B-1 visas allow Mexican drivers to haul freight between Mexico and the U.S., but not within the United States. When B-1 drivers haul domestic freight, it is called cabotage, and it is illegal. This underhanded practice exploits Mexican drivers, and it is unfair to law-abiding motor carriers and American truck drivers. ATA is pushing for stepped-up enforcement against these violations.

Finally, I would like to draw the Subcommittee's attention to a transportation security lapse within the Department of Defense that was identified by ATA's Government Freight Conference. The Department is improperly awarding shipments to unauthorized carriers to move sensitive cargo like M1 Abrams tanks and Bradley Fighting Vehicles.

This practice compromises safety by putting military freight in the hands of unvetted carriers and drivers. Last year, ATA worked with Congress to enact several provisions in the NDAA aimed at this problem, and we will continue to partner with you to shore this up.

ATA thanks the Subcommittee for your interest in identifying foreign ownership risks and hidden vulnerabilities across our transportation system. I look forward to answering your questions.

[The prepared statement of Mr. Spear follows:]



Statement of

**Chris Spear
President and CEO
American Trucking Associations**

Before the

**Committee on the Judiciary
Subcommittee on Oversight
United States House of Representatives**

Hearing on

**“Embedded Threats: Foreign Ownership, Hidden Hardware and Licensing Failures
in America’s Transportation Systems”**

January 21, 2026

Introduction:

Chairman Van Drew, Ranking Member Crockett, and members of the Subcommittee, thank you for providing me with the opportunity to testify before you today. My name is Chris Spear, and I serve as the President and CEO of the American Trucking Associations (ATA). I am grateful for the invitation to share with this subcommittee the growing challenges that our members, the trucking industry, and our nation's supply chain are experiencing with credentialing, fraud, and enforcement.

ATA is a 90-year-old federation and the largest national trade organization representing the 8.4 million men and women working in the trucking industry. As a 50-state federation that encompasses 37,000 motor carriers and suppliers, ATA proudly represents every sector of the industry. From less-than-truckload to truckload carriers, from agriculture and livestock transporters to auto haulers and household goods movers, and from large fleets to mom-and-pop one-truck operators, ATA serves as the single unified voice of the trucking industry.

For the trucking industry, safety is a priority. Ensuring that our roads are safe both for commercial vehicles and the motoring public is our north star. Though commercial trucking is among the most heavily regulated industries in the United States, we continue to see issues that reduce safety and put lives at risk.

Gaps in oversight, enforcement, and qualification requirements—particularly related to English Language Proficiency (ELP), cabotage violations, Entry-Level Driver Training, and commercial driver's license (CDL) issuance—create vulnerabilities that put every part of the trucking industry at risk, from family-owned, small and medium-sized businesses and independent owner-operators to large national motor carriers. These gaps and vulnerabilities are entry points for bad actors to enter the trucking industry, endangering the entire supply chain and the motoring public.

For these reasons, ATA has been working with Congress and the Trump Administration to underscore the urgent need to strengthen driver qualification, training, testing, and licensing standards. ATA has also been forceful in bringing to light issues around the exploitation of cabotage regulations and the issuance and enforcement of B1 visas.

We recognize that failure at any point in this system can not only cause supply chain issues that harm consumers and the economy, but even more importantly, can lead to loss of life or serious injury. We have seen multiple instances this year where a driver of a commercial motor vehicle—who should never have held a CDL in the first place—was involved in a fatal accident. We must work together and expeditiously to enact solutions that will limit these avoidable tragedies.

Thank you for convening today's hearing and providing an opportunity to discuss the challenges that uneven enforcement, lax regulations, and bad actors cause the trucking industry. I look forward to working with this subcommittee, Congress, and the Administration to promote the safety of our nation's roadways.

Critical Vulnerabilities in State Licensing and Driver Oversight

The safety and vitality of America's trucking industry depend on a commercial driving workforce that is fully trained and qualified, thoroughly vetted, and licensed through a system that is uniform, secure, and consistently enforced. However, recent high-profile and tragic commercial motor vehicle crashes, accompanied by nationwide audits, have exposed serious weaknesses in state licensing, driver training, and driver-vetting practices. These incidents are not isolated failures; they are symptoms of deeper systemic breakdowns that compromise the safety and security of our nation's transportation system.

In the wake of recent truck-involved crashes, the U.S. Department of Transportation (USDOT) and its Federal Motor Carrier Safety Administration (FMCSA) conducted a series of federal audits and enforcement actions across all states that exposed significant deficiencies in how some State Driver Licensing Agencies (SDLAs) issue and oversee CDLs, including those issued to foreign, non-domiciled drivers. These failures, ranging from inconsistent verification of lawful status to improper issuance of non-domiciled CDLs, pose real risks to highway safety and to the integrity of our national transportation system. Recent events have also revealed widespread lapses in enforcement of federal English language proficiency (ELP) requirements and exposed the prevalence of noncompliant training providers and fraudulent "CDL mills" that exploit gaps in the Entry-Level Driver Training system.

ATA has long warned that gaps in SDLA compliance and insufficient oversight allow unqualified—and, in some cases, unlawfully present—individuals to obtain commercial driving credentials. These vulnerabilities are compounded when drivers enter the system through training providers that fail to deliver federally required instruction or that certify training which was never completed. When individuals who cannot meet basic ELP standards—or who were inadequately trained—are able to obtain CDLs, it undermines the trust motor carriers and the general public must place in the CDL as a reliable indicator that a driver is properly trained, vetted, and legally authorized to operate in the United States. Insufficient oversight enables illegitimate motor carriers and ill-equipped drivers to exploit loopholes with impunity and operate under the radar.

When the integrity of our nation's CDL system and the regulatory protections that support its integrity break down, the consequences extend far beyond administrative error. They become vulnerabilities that endanger roadway users' safety and can be exploited by bad-faith actors, criminal networks, or foreign entities seeking to commit crimes or disrupt the nation's transportation infrastructure.

The human cost of these failures is indisputable. This past summer, three lives were lost when a commercial driver executed an illegal U-turn on the Florida Turnpike. Investigators later found he had obtained a non-domicile CDL through improper channels and failed to meet basic federal requirements. Just months later, an undocumented commercial driver killed three more victims in a multi-vehicle, chain-reaction crash when he failed to stop. These and similar crashes have pointed to the same underlying issues: gaps in driver vetting, insufficient oversight, and inadequate training at the federal, state, and training provider levels.

Non-Domicile CDL Inconsistencies & Commercial Driver Credentialing Irregularities

In April 2025, ATA wrote a letter to USDOT Secretary Sean Duffy emphasizing the need for enhanced oversight and enforcement of states' CDL issuance processes.¹ We raised concerns about credentialing fraud, licensing irregularities, and the ability of unqualified individuals to obtain CDLs through loopholes or lax state processes. In subsequent months, the results of FMCSA's nationwide audits detailed in its interim final rule (IFR) on non-domiciled CDLs confirmed ATA's concerns about the lapses in driver vetting and credentialing.² The Agency's findings showed widespread credentialing irregularities, inconsistent licensing practices, and noncompliance with federal standards.

Specifically, FMCSA's IFR noted the agency "uncovered systemic procedural and computer programming errors, significant problems with staff training and quality assurance, and policies that lack sufficient management controls in the issuance of non-domiciled CLPs and CDLs by multiple SDLAs." These flaws resulted in SDLAs issuing non-domiciled CDLs to drivers whose CDL expiration date extended beyond the time of a driver's legal presence or work authorization in the country (in some cases, up to four years longer than their employment authorization document's expiration). SDLAs were also found to have issued non-domiciled CDLs without validating the driver's eligibility under federal driver application and certification regulations, among other noncompliance issues. The IFR cites a review of a sample of California non-domicile CDLs, which found that one in four licenses analyzed were issued out of compliance with federal CDL qualification and issuance regulations. These findings were significant enough for FMCSA to issue notices of noncompliance to multiple states, including California, New York, and Minnesota, that required immediate correction under threat of withholding federal highway funds.

Such lapses in oversight and administrative errors not only compromise highway safety—allowing potentially unsafe or illegal drivers on our roads and leading to crashes like those in Florida and California—but also erode trust in the legitimacy of a CDL. This hurts *all* motor carriers and commercial drivers. ATA stresses the need for consistent SDLA compliance with federal CDL program requirements, supported by regular audits and meaningful oversight mechanisms. We appreciate that FMCSA addressed many of these issues in its September IFR and applaud the Agency for its rapid, responsive approach. The interim rule, paired with ongoing audits of SDLA practices on both non-domicile and standard CDLs, help preserve the integrity of the CDL credential so motor carriers can trust it as a reliable marker of driver qualification and lawful eligibility. Rules only work when consistently enforced; ensuring that all SDLAs review their current CDL issuance practices and uphold federal requirements—not exclusively for non-domiciled CDLs, but for all CDLs—is critical. ATA also supports FMCSA's directive that states immediately downgrade noncompliant CDLs, restoring integrity to issuance processes and trust in the legitimacy of existing CDLs.

¹ https://www.trucking.org/sites/default/files/2025-04/ATA_DOT%20April%202025%20Enforcement%20and%20CDL%20issuance%20FINAL4-10-25.pdf

² <https://www.fmcsa.dot.gov/newsroom/president-trumps-transportation-secretary-sean-p-duffy-announces-nationwide-audit-states>; <https://www.federalregister.gov/documents/2025/09/29/2025-18869/restoring-integrity-to-the-issuance-of-non-domiciled-commercial-drivers-licenses-cdl>

Enforcement of the English Language Proficiency Standard

In addition to credentialing concerns, ATA's April letter to Secretary Duffy raised the need for uniform enforcement of driver qualification requirements, including a basic proficiency in the English language in accordance with 49 U.S.C. § 31502(b). ATA urged the Agency to review its then-directives related to enforcement of the ELP standard following reports that enforcement of this provision was inconsistent and that the requirement was often misinterpreted. ATA concluded that these inconsistencies—which prompted some roadside enforcement officers to avoid assessing ELP and writing citations altogether—were primarily the result of FMCSA enforcement memorandum #MC-ECE-2016-006, dated June 15, 2016. This enforcement memorandum also removed ELP as a roadside out-of-service violation, meaning a driver could no longer be legally disallowed to resume driving for failing to adequately demonstrate ELP. In addition to recommending the Agency update the enforcement memorandum to ensure that the provision be enforced consistently during roadside inspections and on-site reviews, ATA encouraged FMCSA to work with the law enforcement community, including the Commercial Vehicle Safety Alliance (CVSA), to ensure that proper enforcement action is taken.

The requirement that a driver be able to read, speak, and comprehend English at a basic level is not new and has been on the books since the 1930s. 49 U.S.C. § 31502(b) ensures a driver can adequately communicate with law enforcement and the public in the case of an emergency or during a roadside inspection. Officers' ability to thoroughly inspect an up-to-80,000-pound vehicle depends heavily upon their ability to communicate with that vehicle's operator. When that communication breaks down or is entirely impossible, roadside enforcement personnel may not be able to get an adequate picture of a vehicle or driver's compliance with federal safety requirements and capacity to continue operating safely. ATA also became aware of instances in which inspectors bypassed trucks whose operators could not communicate effectively in English—allowing potentially unsafe or otherwise illegitimate operators to fly under the radar. Further, a driver's inability to read and comprehend road signs, including dynamic messages that signal inclement weather, compromised road conditions, or oncoming traffic, put the safety of all who share the road in jeopardy.

Within weeks of ATA's letter, President Donald Trump issued an Executive Order, "Enforcing Commonsense Rules of the Road for America's Truck Drivers," which directed USDOT to issue updated guidelines to strengthen ELP enforcement for commercial truck drivers, among other directives. The Agency issued new guidance on May 20, 2025, that reinstated ELP as an out-of-service violation and set forth assessment standards for law enforcement to determine a driver's English proficiency. The two-part assessment includes an initial verbal interview that tests a driver's ability to communicate basic information, such as trip origin and destination or information about a driver's vehicle and equipment, followed by a test of road sign comprehension.³

³ https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/2025-05/FMCSA%20ELP%20Guidance%20with%20Attachments%20Final%20285-20-2025%29_Redacted.pdf

ATA commends the Administration’s actions and welcomes steps toward ensuring safety and accountability on our nation’s highways. Failing to enforce these standards puts lives at risk. While ATA recognizes that most professional drivers meet these requirements and legitimate motor carriers take steps to ensure they hire in accordance with the law, allowing bad actors to bypass existing requirements undermines the credibility of the entire system. Since the enactment of the new guidance on April 25, 2025, out-of-service violations for ELP have totaled over 7,394.⁴ ATA continues to emphasize the need for uniform enforcement of ELP across all states and enforcement jurisdictions, as well as the need for codification of ELP as an out-of-service violation to ensure consistency across future administrations and USDOT leadership.

Noncompliant & Fraudulent CDL Training Providers

Another critical factor when considering the ability and qualification of a driver to operate a CMV safely is how and from whom they receive training. ATA has long supported the Entry-Level Driver Training program, which sets minimum federal standards for those seeking a CDL to ensure consistent classroom and behind-the-wheel instruction regardless of the driver’s state or training provider. Entry-Level Driver Training, which took effect on February 2022 after a multi-year negotiated rulemaking, also requires that prospective commercial drivers train with *approved* training providers listed in FMCSA’s Training Provider Registry. While ATA believes Entry-Level Driver Training has made a significant, beneficial impact on uniformity and safety nationwide, more work can be done to ensure the integrity of the program as recent reports have uncovered fraud and noncompliance by a subset of registered training providers. ATA has raised concerns that the Training Provider Registry—and its associated self-certification process to be listed in the registry—lacks proper vetting to shield prospective drivers and the motoring public from fraudulent and noncompliant training entities.

These noncompliant training providers—often, fly-by-night companies or “CDL mills”—fast-track CDL applicants with minimal, if any, training. They skirt regulations, offering one- to two-day CDL training programs, taking advantage of prospective drivers who merely seek to obtain education to enter the trucking industry as quickly as possible. ATA believes that, in some cases, these providers serve as a venue for individuals to obtain a CDL simply by paying a fee, circumventing the structured curriculum established by Entry-Level Driver Training. In other cases, unsuspecting “students” walk away, having paid thousands of dollars with little to show for it. Not only do these schools produce unsafe drivers who pose serious risks to the motoring public, but they create an unlevel playing field for legitimate training providers and motor carriers who seek to recruit, train, and hire top-tier drivers.

Last month, USDOT Secretary Sean Duffy removed nearly 3,000 noncompliant training providers from FMCSA’s Training Provider Registry and placed another 4,500 on notice for failing to meet federal standards—nearly half of all registered programs nationwide. Many were cited for falsifying records, skirting curriculum and instructor requirements, or refusing to cooperate with federal audits.

⁴

https://ai.fmcsa.dot.gov/EnforcementPrograms/Inspections?type=AllViolations&time_period_id=2&report_date=2025&vehicle_type=1´_critical=19&state=NAT&domicile=ALL

Unfortunately, ATA has been informed that several noncompliant training entities are likely to remain on the Training Provider Registry.

We believe FMCSA must maintain or enhance safety monitoring, auditing, and enforcement actions over the long-term to ensure that unlicensed and unqualified entities are immediately removed from the Training Provider Registry—and new ones are never allowed to enter in the first place. In addition, we have encouraged FMCSA to better track where and by whom drivers are trained and establish triggers when a training entity has reached a certain threshold of driver violations and/or CDL test failures. ATA's Trucking Association Executives Council (TAEC), which is comprised of state trucking association and industry association executives from across the country, similarly called for enhanced monitoring and enforcement of Entry-Level Driver Training providers. Specifically, TAEC stressed the importance of adding Entry-Level Driver Training provider, driving school, and examiner data to individual CDL records, which would enable objective analysis of training and testing effectiveness based on a driver's on-road performance.⁵ TAEC also recommended documenting a driver's progression from Entry-Level Driver Training through testing, permitting, and CDL issuance to identify entities that may be fast-tracking individuals beyond what would be reasonably expected for an entry-level driver.

Additionally, we believe Congress can work with industry partners on commonsense legislation to bolster the efforts of this Administration.⁶ For example, the self-certification process that has allowed so many fraudulent or otherwise unfit training providers go unnoticed should be examined and overhauled. Greater penalties should exist for those who profit from selling sham training and ultimately make our roads less safe.

Supporting a Holistic Approach to CDL Credentialing and CMV Safety

In October 2025, ATA sent a letter to Congressional leadership that highlighted the urgent need for several specific steps towards strengthening the processes and checks that ensure a commercial driver is fit to operate on our nation's roadways. ATA recommended a series of additional targeted reforms to further reinforce CDL testing and issuance standards and strengthen the broader safety framework around commercial driver qualification and vetting. The industry has identified several strategies to support this effort. ATA's full set of recommendations to Congress include:

1. **Codifying the President's ELP Executive Order for truck drivers.** This would ensure consistent, enforceable standards across all states and eliminate gaps in interpretation or implementation. It would also prevent ELP from being removed from the out-of-service (OOS) criteria in the future.
2. **Directing FMCSA to initiate a rulemaking requiring a standardized ELP test as part of the CDL issuance process.** This test could be integrated into existing components of the knowledge or skills tests or implemented as a standalone portion of the CDL examination. A standardized

⁵ <https://truckingresurgence.com/#plan>

⁶ <https://dailycaller.com/2026/01/12/opinion-shut-down-cdl-mills-because-lives-depend-on-it-chris-spear/>

ELP test will prevent a patchwork of SDLA testing approaches and thwart enforcement discrepancies once CDL holders are on the road. Guaranteeing drivers can read and understand road signs, communicate with enforcement officials, and respond effectively in emergencies is foundational to safety. Ensuring these checks are in place at the entryway to obtain a CDL prevents unqualified drivers from ever entering the driving workforce while easing enforcement challenges.

3. **Requiring individuals to hold a standard driver's license for at least one year before becoming eligible for a CDL, with limited exceptions for certain workforce training programs.** This would ensure drivers have sufficient baseline experience operating a motor vehicle before taking on the greater responsibility of driving a commercial truck. FMCSA should provide flexibility and exceptions for certain individuals seeking to enter the driving workforce, such as young drivers, those entering well-vetted carrier training programs, and underprivileged individuals who may lack the means to obtain a driver's license, provided equal or greater training and safety protocols are in place.
4. **Strengthening federal and state oversight of CDL issuance and testing to ensure only fully qualified drivers enter the industry.** FMCSA should expand audits of state driver's license agencies to examine all CDL issuance practices, enforce verification of all federal qualification standards before issuance, and impose penalties on states that fail to comply. In addition, the USDOT Office of Inspector General should broaden its audits to include third-party testers and the Training Provider Registry, ensuring compliance with Entry-Level Driver Training requirements and rooting out improper licensing practices.
5. **Expediting the removal of noncompliant training providers from FMCSA's Training Provider Registry.** States should have the authority to identify and suspend bad actors, while FMCSA should conduct regular audits of Training Provider Registry participants and enforce meaningful penalties for noncompliance.
6. **Strengthening enforcement and penalties against illegal cabotage.** Direct USDOT and the U.S. Department of Homeland Security (DHS) to coordinate and enhance monitoring and enforcement of cabotage violations, including the use of data-sharing between federal and state agencies to track and identify illegal freight movements by foreign-domiciled carriers. Congress should also establish meaningful penalties—such as fines, disqualification, or loss of operating authority—for carriers found to be repeatedly violating cabotage restrictions. Ensuring that only qualified, compliant operators move domestic freight protects highway safety and preserves the integrity of U.S. carrier operations. By focusing enforcement actions on a relatively small group of motor carriers that are engaged in these practices, DHS and USDOT can send a strong deterrent message that reverberates across the industry.

As this subcommittee examines foreign ownership risks and hidden vulnerabilities across transportation systems, it is essential to recognize that lapses in state licensing practices and driver vetting, which have led to thousands of misused CDLs, are part of the same ecosystem of systemic exposure. A compromised system creates openings for individuals who should never be behind the wheel of a

commercial motor vehicle. ATA believes that restoring integrity to CDL credentialing and driver qualifications through consistent enforcement, mandatory employer notification systems, stronger English-language proficiency standards, and rigorous vetting of training providers is foundational to protecting both national security and roadway safety.

Legislative Opportunities to Bolster Progress

There is an opportunity for Congress to take decisive action and build on USDOT's ongoing efforts to restore nationwide uniformity, improve the integrity of driver vetting and credentialing, and rebuild public confidence in the safety and reliability of the commercial driving workforce. As Congress begins consideration of a surface transportation reauthorization this year, ATA further recognizes and supports numerous legislative efforts that aim to protect highway safety and reinforce the integrity of the CDL system, including:

- **Connor's Law (H.R. 3608/S. 2991)**, which would codify President Trump's Executive Order requiring CDL drivers to maintain a basic proficiency in English to be licensed to drive on American roads. This bill includes an out-of-service provision, which would revoke CDL licensure from any current license holders who fail to adhere to language requirements.
- **EO 14286 Act (H.R. 3799)**, which would codify the Executive Order issued by President Trump mandating stricter enforcement of existing ELP requirements for commercial truck drivers to improve road safety. The bill would establish out-of-service penalties for violations and would require a review of foreign-issued licenses.
- **Safer Truckers Act (S. 2690)**, which would establish lawful U.S. residency requirements for CDLs and require states to report adherence to English proficiency standards to ensure truckers can read road warnings and signs, or risk federal funding.
- **Non-Domiciled CDL Integrity Act (H.R. 5688)**, which would terminate states' ability to grant CDLs to illegal immigrants who lack the English proficiency and road-rule knowledge necessary to safely operate CMVs. The bill aligns with the USDOT Interim Final Rule, "Restoring Integrity to the Issuance of Non-Domiciled Commercial Driver's Licenses."
- **Safe Drivers Act (H.R. 5800)**, which would require FMCSA to develop a uniform English proficiency test to be administered during CDL issuance and renewal in every state. The test assesses an applicant's ability to read road signs, understand spoken instructions, and complete written reports. The Secretary of Transportation would be authorized to withhold federal highway funds from states that fail to comply.

ATA looks forward to working with Congress and USDOT to implement comprehensive solutions to ensure consistent compliance with federal driver qualification and CDL-program requirements, reinforced by regular audits, transparent reporting, and meaningful federal oversight.

Electronic Logging Device Fraud as an Emerging Safety and Security Threat

While the integrity of the CDL system is foundational to highway safety, the systems that monitor driver compliance and enable uniform roadside enforcement are equally critical. In recent years, the proliferation of fraudulent, manipulated, or noncompliant Electronic Logging Devices (ELDs) has emerged as a serious and rapidly evolving threat to both roadway safety and the security of the nation's transportation network. ELDs are intended to provide an objective, tamper-resistant record of a driver's hours-of-service (HOS) compliance. When functioning properly, they help prevent fatigue-related crashes, support fair competition, and ensure that carriers and drivers operate within federal safety limits. But the growing presence of devices that can be altered, remotely manipulated, or intentionally designed by foreign enterprises to evade federal requirements has undermined the very purpose of the ELD mandate.

A core vulnerability stems from the current regulatory framework, which allows ELD companies to self-certify their devices through an online registry process. This system enables foreign-owned or overseas-based companies to register, market, and supply devices with weak cybersecurity protections, opaque ownership structures, and remote-access capabilities that blatantly disregard federal ELD regulations and protections. In some reported cases, these foreign actors—posing as legitimate ELD providers—have been able to make real-time edits to drivers' HOS logs at the request of drivers or motor carriers. This can occur within minutes of a driver being pulled over for an inspection and generated using artificial intelligence (AI), producing fraudulent HOS logs that, to the naked eye, appear entirely compliant and legitimate. These capabilities effectively mask hours-of-service violations, compromise regulatory oversight, and allow unsafe operators to continue driving.

The sophistication of these fraudulent actors makes detection extraordinarily difficult. Illicitly edited logs often appear fully compliant unless a roadside officer undertakes extensive cross-referencing with other documentation, such as fuel receipts or toll records. However, it has also come to our attention that some fraudulent entities can produce supporting documentation—fuel and food receipts, for instance—using AI, further complicating vetting of a driver's electronic logs. This remote and illegal manipulation enables fatigued or unsafe drivers to remain on the road, potentially allowing criminals and exploited drivers to fly under the radar. It simultaneously poses a real security threat to logistics infrastructure. Devices with foreign remote-access capabilities could, in the worst-case scenario, provide adversarial actors with visibility into fleet movements, operational patterns, or sensitive supply chain data.

ATA has warned that the presence of fraudulent or easily manipulated ELDs creates an uneven playing field for compliant carriers and erodes confidence in the federal safety framework. When operators can purchase devices that allow them to cheat, falsify logs, or conceal violations, it rewards unsafe behavior and disadvantages the majority of carriers who invest in compliant systems and prioritize safety. Moreover, the use of foreign-sourced ELD hardware with limited transparency raises broader national security concerns, particularly when these devices have the capability to transmit location, operational, and logistical data to unknown third parties.

The consequences of ELD fraud are still being fully understood; however, federal entities have taken these threats seriously. FMCSA has already announced changes that strengthen the ELD certification and review process for new registrants and revoked dozens of noncompliant devices in 2025. ATA emphasizes the need for stronger oversight of ELD manufacturers already listed in the registry, more rigorous vetting of devices before they are approved, swift removal of noncompliant devices, and mechanisms to hold carriers who use those devices accountable.

ATA strongly supports FMCSA's recent enforcement actions and urges Congress to play a role in expanding federal oversight and enforcement of ELD providers, including but not limited to:

- More rigorous vetting of ELD manufacturers, with particular scrutiny of foreign ownership, data-handling practices, and cybersecurity safeguards.
- Ending self-certification and replacing it with a certification and approval process that includes technical testing and security review.
- Regular audits and spot checks to ensure devices continue to meet federal technical specifications after approval, and swift removal of noncompliant devices and clear guidance to carriers on reinstatement and corrective action requirements.
- Enhanced penalties for carriers and drivers who knowingly use fraudulent or manipulated ELDs.

A secure and trustworthy ELD registry is essential to maintaining the integrity of the HOS system, protecting compliant carriers, and ensuring that fatigue-related risks are minimized. Like CDL issuance, weaknesses in ELD oversight create systemic vulnerabilities that can be exploited by those seeking to evade safety rules—or by foreign actors seeking to access or disrupt critical transportation data. Strengthening the ELD program is therefore not only a safety imperative but a national security necessity.

B-1 Visas and Cabotage

The Mexican trucking industry plays a vital role in USMCA trade. Because U.S.-based truck drivers largely do not drive across the border to Mexico to pick up freight, Mexican drivers often enter the U.S. through the B-1 visa program with loaded trailers. B-1 drivers typically drop loaded trailers at U.S. trucking company terminals in the border zone, then return to Mexico with loaded or empty trailers. Without the services of Mexican-based fleets and B-1 drivers, cross-border freight would grind to a halt.

Unfortunately, this integral component of our international supply chains is often exploited by bad actors. Drivers who hold a B-1 visa are not permitted to haul domestic freight within the U.S., but some U.S.-based carriers encourage Mexican drivers to haul point-to-point within the U.S. so they can charge a lower rate for their services. For instance, when a Mexican driver arrives at a U.S. motor carrier terminal, the driver may be told to park his Mexican truck and get into one of the U.S. carrier's trucks to

haul a load point-to-point in the U.S. This practice of a U.S.-based carrier hiring foreign drivers without the necessary work authorization to haul point-to-point in the U.S. is often referred to as cabotage.⁷

The laws and regulations related to cabotage are intended to protect American drivers and law-abiding carriers from unfair competition. However, unscrupulous motor carriers illegally use B-1 drivers because they can get away with paying them significantly less than U.S. drivers. On top of that, by illegally employing these drivers, fleets can avoid paying benefits and payroll taxes. Cabotage is not a technicality or a minor paperwork violation: it is illegal, exploitative of Mexican drivers, and unfair to law-abiding motor carriers and American drivers. U.S. carriers who flout these rules gain an unlawful competitive advantage, distort the marketplace, and put compliant operators at risk of closure.

The scope of the problem is significant. As the 2019 prosecutions in Nogales, Arizona, demonstrate, this activity generates millions of dollars in illegal revenue for corrupt carriers while hollowing out American jobs. In one case, a company reaped \$2.4 million by coercing unauthorized foreign drivers to haul point-to-point in the U.S., while another netted \$1.3 million before being shut down.⁸ These are not isolated bad actors—they are part of a pattern of willful lawbreaking that undermines the integrity of our supply chain.

U.S. Customs and Border Protection's (CBP) enforcement actions provide insights into how widespread this illegal practice has become. ATA has learned that recent checkpoints established by CBP's Customs Trade Partnership Against Terrorism (CTPAT) Office revealed multiple cabotage violations within the border zone. In fact, the CTPAT Office recently warned motor carriers in the program that violations of cabotage rules would risk CTPAT certification.

Additionally, last year, CBP detained two Mexican truck drivers and seized their commercial vehicles in Arizona after the drivers illegally hauled domestic U.S. freight. CBP officers revoked the drivers' border crossing cards due to violations of their visa terms. These incidents occurred after CBP issued an alert back in May of 2025 reminding U.S. motor carriers of cabotage regulations and the consequences of violations.⁹

Again, it cannot be emphasized enough: legitimate drayage services are essential to cross-border freight, and both the trucking industry and American economy would suffer if this system were to be disrupted. However, ATA strongly supports Federal intervention to stop bad actors who exploit foreign drivers to haul domestic freight. In September of this year, ATA wrote to DHS Secretary Kristi Noem requesting greater enforcement of cabotage regulations.

⁷ While the term cabotage technically refers to foreign carriers providing point-to-point service in the U.S., it is regularly used to describe any point-to-point delivery made by a foreign driver, whether hired by a foreign motor carrier or a U.S. motor carrier. This is how we are using this term.

⁸ Pendergrast, Curt (2019, April 23). *Feds Say Nogales Trucking Companies Illegally Hired Mexican Drivers*. Tucson.com https://tucson.com/news/local/feds-say-nogales-trucking-companies-illegally-hired-mexican-drivers/article_d2c5d8e9-7361-535a-bc69-670c5cabf07f.html

⁹ Fletcher, N. (2025, December 1). *Border Patrol Detains Mexican Truck Drivers for 'Cabotage'*. *Transport Topics*. <https://www.ttnews.com/articles/mexican-truckers-cabotage-us>

One potential tool to deter bad actors from engaging in this type of exploitation is an export manifest, which we know CBP is already considering. Today, there is no practical way of tracking when a Mexican driver leaves the U.S. With the submission of an export manifest, driver information would be recorded just as it is for import manifests. By collecting export data via an export manifest, CBP would be able to identify patterns that indicate potential cabotage violations by B-1 drivers. For example, if a Mexican driver entered the U.S. to haul a load to Laredo, TX, and stayed in the U.S. for three weeks, that would raise a red flag. ATA believes that tracking this data is the first step in drastically reducing cabotage violations.

Department of Defense's Freight Issues

ATA's Government Freight Conference is a group of motor carriers and drivers that proudly transport freight for the U.S. government, including arms and ammunition, combat vehicles, and other sensitive cargo. Department of Defense regulations require motor carriers to register and, as part of participation in the Department's freight program, comply with rules specific to the transportation of sensitive military freight (e.g. constant surveillance and custody of a shipment, unique training for drivers, the use of specialized equipment, and employing drivers with security clearances.) These requirements are commonly referred to as Transportation Protective Services. In 2024, the Department proposed to waive these important services to increase capacity during a "surge" in shipments of arms and ammunition. ATA opposed the proposal, arguing that allowing unqualified carriers and drivers to haul munitions that have little or no experience in hauling this sensitive, dangerous commodity was an unnecessary risk to national security and highway safety. The Department was intent on moving forward with its policy change, so ATA worked with Congress to enact a prohibition as part of the National Defense Authorization Act (NDAA) for FY25 [P.L. 118-159, Section 852].

In recent years, the trucking industry has shared data with the Department that indicates systemic waste, fraud, or abuse within certain segments of its transportation program, and we have attempted to work collaboratively with the Department to address these issues. In many cases, military shipments are awarded to service providers that are not authorized to transport sensitive freight or cannot meet the service requirements. In other words, the Department is awarding shipments to unauthorized carriers to transport M1 Abrams tanks, Stryker and Bradley fighting vehicles, and other armored vehicles across our nation's highways and onto our military installations. This undermines the viability of the Department's legitimate trucking capacity that has invested in the training and safety protocols to ensure these commodities are transported safely. Moreover, this practice compromises the safety and security of some of our military's most sensitive cargo by putting it in the hands of unvetted carriers and drivers with unknown intentions.

To begin the process of eliminating this vulnerability, ATA worked with Congress last year to enact several provisions in the FY26 National Defense Authorization Act. Included in the FY26 NDAA were: (1) an audit of the Department's Freight Carrier Registration Program (FCRP) to ensure service providers have active USDOT operating authority, (2) an update of the FCRP to ensure service providers are clearly listed as a motor carrier or broker, (3) Global Freight Management training for transportation officers and service providers, and (4) a process for stakeholders to notify the Department of potential violations of policy. These provisions are intended to ensure that authorized carriers are using qualified drivers to transport sensitive military freight. ATA looks forward to working with Congress and the Department to continue ensuring that the military's most sensitive freight is transported by service providers who are qualified to move those goods safely.

In Conclusion

Chairman Van Drew, Ranking Member Crockett, and members of the subcommittee, thank you again for the opportunity to testify on behalf of the American Trucking Associations.

An unwavering commitment to safety is at the core of ATA. We firmly believe that the CDL should represent a promise to everyone sharing the road that the person behind the wheel of an 80,000-pound vehicle is qualified, competent, and accountable.

Unfortunately, years of lax and uneven enforcement at both the federal and state levels have undermined that promise. As I laid out in this testimony, systemic breakdowns in the systems that manage driver training, state licensing, carrier vetting, and cross-border trade pose significant threats to the supply chain and the motoring public. Bad actors and negligence expose these faults.

But as this testimony has also laid out, solutions exist. Some are already being implemented. Our industry is encouraged by Secretary Duffy's clear understanding that safety is trucking's North Star, and we appreciate Congress' attention to this issue.

Further steps can be taken to build on this progress. States must strengthen their verification systems. Federal agencies need to remain vigilant by enforcing existing regulations or considering new ones. Congress should work with industry partners on commonsense legislation to bolster the efforts of this administration.

We must secure these systems to maintain a qualified workforce in the trucking industry, not only to protect the supply chain, but to protect the motoring public. There are ways to effectively administer state licensing, driver training and vetting, and cross-border trade while still providing opportunities for qualified drivers to work in our industry.

This isn't about politics. Highway safety is not a partisan issue. Truck drivers, motorists, families, and businesses all benefit when standards are enforced and bad actors are removed from the system.

Truck drivers are professionals, and the public deserves to know every CDL holder has earned that title. Lives, American jobs, and our national security depend on it.

Mr. VAN DREW. Thank you, Mr. Spear.

Mr. Rob Knake is the Chief Executive Officer of TPO Group, a cybersecurity consulting firm. He previously served as the Deputy National Cyber Director with the National Security Council and at the Department of Homeland Security.

Mr. Knake?

STATEMENT OF ROB K. KNAKE

Mr. KNAKE. Thank you, Chair Van Drew, and thank you, Ranking Member Crockett and the Members of the Committee, for the opportunity to testify on this subject.

While I can't speak to the issues that my colleague Mr. Spear has addressed, I think you are going to find that the bipartisan approach that you were hoping for, Chair Van Drew, really has emerged, at least within the cybersecurity community, on these topics. There is very little that I could disagree with in either the tone or the substance of what my other two panelists have said about the cyber threats.

As not to repeat much of what they have said, let me make a series of points about how we address these threats. First, let me applaud the focus on embedded threats. As Mr. Cole pointed out, our critical infrastructure is compromised through remote hacking capabilities that China, Iran, Russia, and North Korea have deployed. This is a serious issue. This is a serious risk, and more needs to be done to address that traditional threat.

The threat from embedded systems that are dependent on Chinese-produced electronics, Chinese IT components, and Chinese products is unique to China because of the scale of their manufacturing and the lack of capacity that we have in the United States today.

I will primarily focus my remarks on the cyber aspects here, but it should be noted that in the event of a conflict with China, they will have the ability to cutoff supplies for critical minerals, critical goods, critical parts, and services that our economy needs to run. That alone means that we need to diversify our supply, onshore our supply, and build trusted supply networks with our allies overseas.

While we need to diversify our supply, we also simply cannot simply trust that something produced by an ally or something produced by a U.S. company, built by U.S. citizens, is necessarily trusted. Let me go for another point of bipartisanship here by quoting Ronald Reagan. This is an area where the mantra needs to be, "Trust but verify."

We need to verify that the systems we rely on are in fact secure, regardless of whether they are produced by a U.S. company from entirely U.S.-made components or they are produced by our allies through an extended and secured supply chain. We cannot simply assume that onshoring will address this risk.

We have seen the risk from transshipment where U.S. companies may think that they are building from chips that did not in fact come from China, but those chips may have been transshipped from China through Vietnam, Mexico, or another country. A drone or other device that you may think is secure and is U.S. and American made may have a risk inside it that even the company that manufactured it does not know about.

That is why it is critically important that we invest in the ability not only to produce these goods domestically and with our allies but also be able to identify and recognize when these supply chains have been compromised and when there are back doors or logic bombs or other threats embedded in these systems. We can envision a future in which we have trusted supply chains, but to get there, we need much stronger government action.

Chair Van Drew, to your point about a more expensive Chinese system, I think what we are seeing today is that, typically, Chinese suppliers are often cheaper, but in some cases they in fact have better capability than some U.S.-produced goods. What that will mean on the market is that companies are going to purchase the cheaper good, particularly if it is more effective than an American-made good.

I was part of a long-running—what I would call a whispering campaign against Huawei to say that Huawei's technology shouldn't be trusted; it shouldn't be put in our core infrastructure. The FBI did briefings. We did briefings at the NSC. What finally worked was banning that technology, and then for the rural broadband telecommunications providers that were incapable of investing to replace that, subsidizing that investment.

We need a far broader approach like that to the categories of technology that China is dominant in today, and we need to develop and invest in the ability to verify that the replacement technologies produced in the United States are, in fact, secure and have not been compromised.

Thank you for this opportunity.

[The prepared statement of Mr. Knake follows:]

40

Testimony of
Robert K. Knake

Before

The U.S. House of Representatives
Subcommittee on Oversight
of the Committee on the Judiciary

**“Embedded Threats: Foreign Ownership, Hidden Hardware,
and Licensing Failures in America’s Transportation Systems”**

Wednesday, January 21, 2026
2:00pm

Room 2141
Rayburn House Office Building

Introduction

Thank you Chairman Van Drew and Ranking Member Crockett, and Chairman Jordan and Ranking Member Raskin, and members of the committee for giving me the opportunity to testify at this hearing on Embedded Threats: Foreign Ownership, Hidden Hardware, and Licensing Failures in America's Transportation Systems. I strongly agree with the conclusion that there is an urgent need for additional federal oversight to protect national security and public safety on this topic and will share with you my perspective on why this is necessary and what should be done, drawing on my experience as a researcher, a policy maker, and an investor. While I am drawing on these experiences, let me be clear that I am testifying in my personal capacity.

When it comes to foreign threats to our critical infrastructure, for the purposes of this hearing on foreign ownership and supply chain risks, China and Chinese manufactured products and components are by far the greatest risk. This is not to down play the risk from Russian cyber adversaries that have used software supply chain attacks (most notably the 2021 SolarWinds incident) to compromise even the most hardened targets or the risk posed by North Korean technology workers that have gained access to US companies posing as legitimate remote workers, but these risks pale in comparison to the risk from Chinese electronic systems and components and the software embedded in them. On this basis, I will focus my remarks on understanding this risk, highlight potential avenues for addressing this risk, and provide my thoughts on how the government can shape market forces so that the owners and operators of our critical infrastructure will be positioned to reduce the risk.

Understanding the Risk Posed by Foreign Ownership and Embedded Systems

Broadly speaking, the risks posed by foreign ownership of our critical infrastructure are not nearly as dangerous as the risks posed by untrusted and unverified hardware and software components that our critical infrastructure relies upon. I may not love the fact that my local utility, Central Maine Power, is owned by the Spanish energy giant Iberdrola or that the profits from each kilowatt hour I buy are returning to Canadian pensioners through their investment, but given both the oversight on these investments as well as the strong regulatory framework around the bulk power system, the simple fact of foreign ownership is not high on my list of risks. Given the heightened scrutiny on these investments and the programs put into place to address these risks, there are circumstances under which the US government has set a higher bar for oversight and more stringent security requirements than for an American owned company. While I do not intend to minimize the risks posed by foreign ownership, the far greater risks come from foreign operation of our critical infrastructure and reliance on foreign software and hardware. And, of course, that risk is principally from China given their dominance as a supplier of many critical electronic systems and their status as a near peer adversary.

As the “typhoon” campaigns have shown, China has dedicated considerable resources to gaining access to our critical infrastructure with the intention of being able to disrupt it in the event of conflict with the United States. Based on publicly available information, my understanding is that these campaigns did not rely on compromising the supply chain but instead gained access through remote hacking techniques. That our critical infrastructure remains vulnerable through these attack pathways is unacceptable. This risk can be managed with increased investment, improved vigilance, and increased collaboration with government agencies. It will require improved oversight and is by no means a solved problem but managing this risk is also not beyond the capability of our critical infrastructure owners and operators and the national security apparatus of the United States. The risk from our supply chain dependence is one that we have known about for a long time but are just now beginning to grapple with.

It is important to emphasize that cybersecurity is a process of ongoing improvement – it is never a finished project. That is because our adversaries – whether criminal organizations or nation states – are not going to simply give up. We must anticipate that if we are able to prevent our adversaries from gaining access to our critical infrastructure through phishing campaigns, stolen credentials, and exposed vulnerabilities, they will use other means to attempt to achieve their objectives. We can and should anticipate that in a moment of heightened geopolitical tension, China will have the ability to cause disruptions to the operation of our critical infrastructure due to the scale at which we are reliant upon Chinese produced systems and components. Through a combination of executive actions and bills that Congress has passed, we have taken steps to address concerns with specific companies such as Huawei, TikTok, and now the drone company DJI. Yet we still lack a comprehensive regime to evaluate the risk of Chinese produced products and components and determine how to mitigate that risk.

Developing Trust in Our Supply Chains

There is no escaping the fact that China is our third largest trading partner and a critical supplier of everything from textiles to telecommunications equipment. Yet it is by most accounts a trade partner that we cannot trust. While efforts are underway to bring back American manufacturing and develop international supply chains that do not run through China for critical goods, given the scale of US demand we should anticipate that we will continue to source many goods from Chinese companies for years to come. Some goods, like textiles, pose little risk. But for our critical infrastructure, we must recognize that this trade relationship creates the potential for China to disrupt our critical infrastructure either by compromising equipment at the point of manufacture or simply by cutting off supplies of critical components at a moment of heightened geopolitical tension.

It is therefore a matter of national security that for our critical infrastructure, military, and government systems, we develop trust in our supply chains at every level. At Paladin Capital

Group, where I am a Venture Partner, we have worked with twenty other like-minded investment firms to develop the concept of Trusted Capital and articulated a set of Investment Principles and Commitments on Trust, Safety, and Security. These commitments include ensuring that the companies we invest in: 1) invest in their own security to protect themselves against the risk of being compromised by our adversaries; 2) build safe and effective software by implementing appropriate secure-by-design and resilient-by-design principles and are taking affirmative steps to identify and mitigate risk both prior to and while their products are deployed; 3) take affirmative steps to identify and mitigate risks in their software supply chain; and 4) encourage and incentivize the responsible discovery and reporting of vulnerabilities and engage in rapid remediation of identified vulnerabilities.

These principles are also, of course, a roadmap for investment. More investment is needed to develop technologies to detect and thwart our adversaries, build safe and effective hardware, detect risks in supply chains, and improve vulnerability discovery and remediation. More work needs to be done to both produce secure software and identify vulnerable or malicious code and vulnerable or compromised hardware components. It remains difficult but not impossible to identify vulnerabilities in the millions of lines of code that comprise modern software; likewise, it is difficult but not impossible to identify counterfeit or otherwise compromised hardware components. More research and development is sorely needed in these areas.

Given the subject of this hearing, I would like to take a minute to focus on the importance of improving transparency in our supply chains. In order to secure our critical infrastructure, we must know where the software and hardware they rely on come from – who owns it, who produced it, who has access to it and can control it. To help answer these questions, Allan Friedman, a colleague of mine at TPO Group and at the Institute of Security and Technology (IST), has shepherded into existence the Software Bill of Materials or SBOM while serving at the Commerce Department and then the Cybersecurity and Infrastructure Security Agency (CISA). Now, he is working to create the same level of transparency for hardware through development of a Hardware Bill of Materials or HBOM.

There is immense value to be gained from traditional approaches to Third Party Risk Management that look at suppliers from an external perspective. Indeed, adversaries will always gravitate toward exploiting a known vulnerability to meet their objectives before they will burn a zero day or undertake a supply chain attack. But multiple incidents in recent years have underscored the dangers from industry-wide reliance on fundamentally insecure software. To quote Dr. Friedman, much of the software we rely on to make modern life possible is built on “a foundation of sand” – software assembled from open source that is then compiled and then forgotten only to be discovered once an adversary exploits it. SBOMs, now a ten-year-old concept, serve as a “list of ingredients,” allowing buyers to feel confident that manufacturers are using the freshest quality components. There are free tools that any company can use to produce

an SBOM and there are dozens of US companies that will help software makers produce and manage them. In short, there is no reason why a software maker cannot produce the equivalent of an ingredients list for their customers today. Armed with this information, when a new vulnerability inevitably emerges, we can much more easily understand the risks that it presents, who is affected, and how to prioritize remediation.

We need the same level of visibility for hardware and that is still a work in progress today. Modern electronics systems use many different semiconductor components and, unfortunately, far too many of those chips are built in China. The first step to understanding this risk is, again, transparency. Customers need a more thorough understanding of the hardware components that comprise the systems on which we all depend. While eliminating all Chinese chips from all electronics systems today may not be feasible, we can start to ask for a more careful accounting on what chips are used, and the trustworthiness of their origins. For more critical applications, like what we are discussing today, we want to select trustworthy manufacturers (i.e. American companies and American manufacturers using chips and components from trusted suppliers).

This won't solve everything—we will still need security researchers, including our National Labs, to identify undocumented risky hardware capabilities and vulnerabilities. But with expanded use of SBOMs and the further development of HBOMs, it will be easier and cheaper to detect and respond to newly identified risks, and manufacturers will have a greater incentive to seek out trusted hardware components from America and her allies.

Shaping Market Forces to Value Security

While I am excited by many of the technologies coming to market to address these risks, they will only be deployed if the owners and operators of critical infrastructure are required to achieve security outcomes. One of my major takeaways after working on these issues for nearly three decades is that the level of investment in security that may make sense for a company to manage its own risks is often far lower than the level of security required to address national security risks. Thus, the government must intervene to shape markets through a combination of informing risk, setting requirements, and where necessary, subsidizing security investment. We should not rely on the individual patriotism of our corporate leaders but instead shape markets to value and invest in security so that the imperative of maximizing corporate value does not run counter to but is aligned with our national security.

I am a strong advocate for regulations that are outcome based and efficiently enforced. In developing the last National Cybersecurity Strategy, my team at the Office of the National Cyber Director placed heavy emphasis on the need to harmonize regulation so as to reduce the burden on our partners in the private sector. I am pleased to understand that this goal, embedded in

ONCD's statutory language, will be doubled down on in the Trump Administration's forthcoming cybersecurity strategy.

Where a lack of regulatory harmonization most impacts regulated entities and costs companies time and money that could be better spent on actually implementing security is in examination and enforcement. Drawing on the same set of requirements is good but regulators often will interpret these requirements differently. A practice that is acceptable to one may not be acceptable to another. This risk is very real in the transportation sector where at an intermodal facility, for example, TSA may have oversight of pipelines, the Coast Guard may have oversight of shipping, and FERC may have oversight of energy elements. Coordinating this enforcement through a tiger team approach for each company or facility can improve security outcomes and reduce costs for the regulated entity.

For supply chain security, coordinated and direct Federal regulation is often preferable to third-party approaches that make regulated entities the regulators of their supply chains. To underscore this point, let me relay an anecdote from my time developing the last National Cybersecurity Strategy. Early on in the process, as we began outreach to our private sector partners on this topic, the Director received a request for a phone call with the CEO of one of America's largest financial institutions. I joined the call as did the financial institution's CISO. He did not get a word in edgewise. Clearly speaking without the aid of any notes, the CEO relayed the costs and difficulties of attempting to meet the requirements of his regulators to regulate his third-party suppliers, particularly the hyperscale cloud providers that his company relied on. While he fully recognized that his dependence on these providers created a risk that required oversight, he argued convincingly that even at the scale he was purchasing cloud services, his business was not critical to these providers, and he could not effectively compel change. He argued that instead of passing down requirements, the hyperscalers should be directly regulated – his CISO should be responsible for implementing security controls for the applications they built and deployed in the cloud but he should not be responsible for assuring the security of the technology stack at the hyperscaler upon which thousands of companies rely.

Within the same week, I fielded a call from the CISO of one of these hyperscale cloud providers. Approaching the topic from the perspective of a vendor that was being managed as a third-party, his frustration was multiplied by the fact that he was dealing with several dozen financial entities that were required by their regulators to conduct diligence on his security as well as direct examination by several of the regulators themselves. Surprisingly, he had come to the same conclusion as the bank CEO – that it would be better for both him and his customers if the government directly addressed the supply chain concern. He noted that his company was fully compliant with FedRAMP up to and including FedRAMP High. He asked why if FedRAMP was sufficient to assure mission critical government systems, it was not sufficient for the financial sector. And, indeed, if it was not sufficient, he strongly suggested that fixing it rather than

establishing parallel oversight and enforcement would be in all parties' interest. I strongly support this position and applaud the efforts of the FedRAMP team to both speed up the current process of FedRAMP approval and the move to a real-time telemetry-based approach. In future years, I strongly support including requirements for SBOMs and HBOMs. Doing so will provide necessary transparency and improve assurance of the vital software applications and infrastructure that all sectors, including transportation, rely on.

Leveraging Market Forces through Catastrophic Bonds

As I testified in 2019, I believe that cyber insurance, particularly catastrophic bonds, can and should be used as a mechanism for companies to internalize national security risks by requiring that they have the financial resources to make victims whole in the event of a catastrophic loss. My longtime colleague Dr. Stephen E. Flynn, the director of Northeastern's Global Resilience Institute, and I have advocated for an insurance model that would promote risk reduction rather than just risk transference. Dr. Flynn, a retired Coast Guard officer, has posited that the regime put in place under the Oil Pollution Act of 1990 after the Exxon Valdez oil spill could be ported over to secure our critical infrastructure from cyber attacks -- in other words, we should treat data spills like oil spills. Under the regime put in place to prevent oil spills, ships entering U.S. waters must provide proof in the form of a Certificate of Financial Responsibility that their owners or their guarantors in the insurance industry have the financial resources to cover the cost of cleaning up an oil spill should containment on their vessel fail.

Notionally, owners of critical infrastructure could be required to take out insurance policies to cover the full societal cost should they fail to protect the infrastructure for which they are stewards of. Congress could establish a process to determine required coverage levels and then require owners and operators of critical infrastructure to obtain coverages in these amounts. From there, market mechanisms would take over to determine how to price risk. For instance, if natural gas pipeline owners had to obtain private insurance to cover the costs of a disruption to service caused by malicious cyber activity, markets would likely require a far higher degree of assurance than would be required through a standard regulatory model.

Strengthening the Governments Role as a Partner

Given the subject of this hearing, I have placed greater emphasis on the government's oversight role but no less important is government collaboration with our critical infrastructure owners and operators. Let me be clear that, contrary to popular wisdom, government regulation does not preclude voluntary collaboration. In fact, the strongest public-private collaborations on cybersecurity are with the most heavily regulated industries. If private sector entities must achieve security outcomes, the government is an invaluable partner. While the primary responsibility for protecting systems and assets lies with the owners and operators of those

systems and assets, there are things that only the government can do to counter threats such as gather intelligence, carry out offensive cyber operations, and shape adversary behavior through sanctions and diplomacy.

Public-private collaboration has improved immensely over the last decade, having shifted from annual or quarterly meetings to real time collaboration on emergent threats with many of our most critical companies. Continuing to strengthen these mechanisms should be a priority for Congress and the Administration. When it comes to supply chain risks, collecting intelligence on adversary attempts to compromise products and components must be a priority. Moreover, sharing this intelligence with our partners in the private sector must become both faster and more routine.

Conclusion

Thank you for the opportunity to testify on these important issues. I look forward to continuing to engage with you, your staff members, and with my colleagues in the executive branch to develop law and policy to address these risks. I would be happy to answer any questions at this time.

Biography

Rob Knake is the CEO of TPO Group, a boutique cybersecurity consulting firm, and a Venture Partner at Paladin Capital Group. He is also a Senior Policy Advisor at the Institute for Security and Technology and a Senior Fellow at the McCrary Institute and an advisor to cybersecurity firms including Anitian, Cyera, Defendify, and Security Scorecard.

Rob served as Deputy National Cyber Director for Strategy and Budget at the Office of the National Cyber Director in 2022-2023, where he led development of the National Cybersecurity Strategy among other matters. In previous government service, Rob served from 2011 to 2015 as Director for Cybersecurity Policy at the National Security Council. In this role, he was responsible for the development of Presidential policy on cybersecurity, and built and managed Federal processes for cyber incident response and vulnerability management.

In previous roles, he was a Senior Fellow at the Council on Foreign Relations and a Professor of Practice and Senior Research Scientist at Northeastern University. He is co-author of *Cyber War: The Next Threat to National Security and What to Do About It* and *The Fifth Domain: Defending Our Companies, Our Country and Ourselves in the Age of Cyber Threats*. He holds a Master's in Public Policy from Harvard's Kennedy School of Government and undergraduate degrees in history and government from Connecticut College and is a life member of the Council on Foreign Relations.

Mr. VAN DREW. Thank you, Mr. Knake. All good statements.

I am going to ask you all to rise to be sworn in. Raise your right hand. Do you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

You may be seated.

Mr. RASKIN. Point of order, Mr. Chair.

Mr. VAN DREW. Yes.

Mr. RASKIN. Does that apply also to testimony they have already given?

Mr. VAN DREW. Correct.

Mr. RASKIN. Thank you.

Mr. VAN DREW. Thank you for that. That does apply to the testimony you have already given. What the Ranking Member is pointing out in his gentle way is I should have done that at the very beginning when you started your testimony.

That is a good point. Thank you.

With that being said, we are going to begin with the questions. I am going to start with the gentleman from Missouri, Dr. Onder.

Mr. ONDER. Thank you, Mr. Chair.

Over the past decade, Federal agencies and infrastructure operators have embedded software-driven electrical equipment throughout America's roads, ports, rail systems, and power networks. Through this rapid modernization, we have quietly opened a dangerous national security vulnerability. Foreign-manufactured hardware now sits at the core of systems that keep the American economy running and the military moving.

Nowhere is the threat more acute than in the power sector. Chinese-made inverters, batteries, and transformers have become foundational to the power grid and critical infrastructure. The components are designed, built, and in some cases remotely controlled by firms operating under the authority and influence of the Chinese Communist Party. As a result, the CCP is increasingly positioned to monitor, disrupt, or manipulate the infrastructure that underpins U.S. commerce, public safety, and national defense.

Ms. de La Bruyère, can you explain why it is inherently dangerous for U.S. roads, ports, and rail systems to rely on electronic components manufactured in China, particularly when those components are embedded deep inside operational systems?

Ms. DE LA BRUYÈRE. Yes. There are three main reasons from the informational perspective.

(1) *The first is those components give China access to critical American information:* Who is traveling, where, when, and how. That is like a personal privacy risk, but it is also a strategic asset.

We are in a competition where data is the new oil. Data is the single most dominant resource. In the great power competition with China, if Beijing has full information on our society, that is how it can target all its attacks.

(2) *China can shape information:* If information is fueling transportation and you can shape information, you can decide who is moving where, when, and what. You can pick winners and losers, what company, shipping route, and software add-on is going to win. That means that Beijing controls our society.

Then, there is the disruption threat. All these two things are short of any outright conflict scenario. That is just happening. If China decides it is time, they can shut off our systems. They can interfere with our systems. They can destabilize our society.

(3) *That is informational threat:* On top of it, there is just a basic supply chain and industrial threat. China can stop providing these components. We are trying to build new infrastructure or modernize infrastructure. We are at their mercy? Plus, our industrial base depends on being able to produce these critical goods. Our country depends on having an industrial base. Our economy depends on that. If we forfeit that to China, there goes American growth and freedom.

Mr. ONDER. What categories of U.S. infrastructure, like EV charging stations, tolling stations, rail signaling, port cranes, traffic management systems, currently depend on foreign-manufactured electronic hardware? I am afraid you are going to say all the above.

Ms. DE LA BRUYÈRE. All of the above. At so many levels, too, that we aren't—you mentioned inverters. No one is talking about inverters.

Mr. ONDER. Right.

Ms. DE LA BRUYÈRE. That is a huge risk to the grid. All of those sectors. Every sector. Data centers. Optical transceiver—building them at rapid scale. Optical transceivers are necessary for data centers. We increasingly depend on those for so many other industries. What if China shuts those off?

Mr. ONDER. Yes. I was at an energy conference in Houston a few months back, and someone, one of the speakers, talked about Chinese-made batteries. Any kind of reliance on so-called green energy when their solar is going to rely on massive battery-charging capability, or even one's—the electrical panel on one's roof, private home, would depend on a battery.

Apparently, a large percentage of these are being made in communist China right now. Those could, in theory, be remotely flipped off or even remotely made to overheat, causing electrical power or even explosion risk.

Mr. Cole, I see you nodding. Any comments on this?

Mr. COLE. Congressman, I was just discussing with the other witnesses before the hearing that there are virtually no cybersecurity standards around electric vehicles as a category, whether that be batteries that can communicate directly, perhaps, with China, or other cybersecurity standards of the self-driving components of the vehicle.

You can imagine a world where the United States is trying to mobilize for a conflict, and suddenly EVs are blocking roads, the interstates, and cities.

Mr. ONDER. Yes. It is frightening. Thank you. I yield back.

Mr. VAN DREW. I thank the gentleman. The gentleman from Georgia.

Mr. JOHNSON. Thank you, Mr. Chair.

Hostile foreign nations like China are targeting critical infrastructure here in America. Donald Trump is enriching himself with money from China while weakening United States programs that protect us from their security threats.

For example, the Chinese Government and its State-controlled entities spent over \$5.5 million at Trump-owned properties during the first Trump Administration. In this second administration, the greed and corruption is turbocharged. A Chinese company recently announced that it would buy up to \$300 million of President Trump's cryptocurrency. Coincidentally, the Trump Administration is systematically weakening our defenses against China's security threats.

Ms. de La Bruyère, would you agree that the U.S. needs to be the No. 1 country for artificial intelligence?

Ms. DE LA BRUYÈRE. I would agree with that.

Mr. JOHNSON. You would agree also that Nvidia chips power the Nvidia or the AI revolution, correct?

Ms. DE LA BRUYÈRE. They are among the components that power the AI revolution, yes.

Mr. JOHNSON. Does it surprise you that Trump has discarded America's strategic technological edge over China insofar as AI chips by changing the rules and allowing the export of Nvidia's AI chips to China?

Ms. DE LA BRUYÈRE. What surprises me the most is that—

Mr. JOHNSON. Does that surprise you?

Ms. DE LA BRUYÈRE. I think what surprises me the most is that we don't actually have an edge in AI chips over China anymore.

Mr. JOHNSON. OK. All right. You want to take me in a different direction.

Ms. DE LA BRUYÈRE. Yes, sir because it is important

Mr. JOHNSON. I don't want to go in the direction you are trying to take me.

I am going to now ask Mr. Cole. Mr. Cole, Elon Musk and his DOGE musketeers benched hundreds of cybersecurity professionals at the Cybersecurity and Infrastructure Agency, also known as CISA, and at the National Security Agency. Nearly a third of CISA's staff was cut, including divisions that coordinated with States and businesses which provide key assistance for transportation infrastructure.

Was that a wise move by Trump?

Mr. COLE. Well, first, Congressman, I'm a native Georgian, so it is a pleasure to meet you.

Mr. JOHNSON. Well, good to meet you, too, sir.

Mr. COLE. I have always wanted to. To answer your question, I do think now is not the time to cut CISA's budget or operational—

Mr. JOHNSON. That was a bad move. His budget request to Congress now includes an additional 18 percent cut to CISA's Cybersecurity Division, which leads efforts to protect government networks and helps defend critical infrastructure. Was that a good move or a bad move?

Mr. COLE. Congressman, if you go around the country and talk to the State cyber leaders, they will all tell you they would like additional Federal support to respond to cyberattacks.

Mr. JOHNSON. Well, it was a bad move. That is probably what you are trying to say.

Let me ask you, Mr. Knake. We have seen our foreign adversaries exploit cyber vulnerabilities against our communications, energy, and water sectors, among others. It may be easy to discount

national security risk to our transportation infrastructure because we haven't yet seen widespread consequences in this field.

While embedded technology like undisclosed radios and batteries in cranes clearly shows that our adversaries may have the capability to conduct espionage or even cause outages in transportation infrastructure, when local governments or private companies are acquiring technology, they may be willing to overlook the national security risk in favor of getting technology that they need more quickly or for cheap, or cheaper.

Does the fact that we haven't yet seen a major cyberattack against our transportation infrastructure mean that we don't have to worry about this national security threat? It comes at a time when Trump's net worth increased by \$3 billion over last year. With this security threat, does it mean we need to be worried, or do we have cause for concern as the President gets richer and our security is eroded?

Mr. KNAKE. Sir, we have absolutely seen campaigns carried out against our transportation infrastructure for the purposes of collecting intelligence and for the purposes of planning future attacks. What we haven't yet seen is significant disruption of that infrastructure because the geopolitical moment in which our adversaries would want to take advantage of that has not emerged yet.

Mr. JOHNSON. Thank you. I yield back.

Mr. VAN DREW. I thank the gentleman.

I am going to yield five minutes to myself. This is to Mr. Spear. How does weakened enforcement of Federal CDL and English proficiency requirements undermine safety on American roads? Tell me if you agree this should be viewed as a national security and rule-of-law issue rather than just a regulatory problem.

Mr. SPEAR. Well, the criteria or the standards that you are speaking to come from the United States Department of Transportation, handed down to the States. The States administer the tests. Some States do it very well, and there is a handful that aren't.

We have seen over the last few years a whole host of CDLs get issued to people that shouldn't have them, candidly. First, they may not be here legally. They may not be able to speak or understand English. They shouldn't be operating an 80,000-pound heavy-duty truck, moving freight across the country.

Those standards and the relationship between the Federal and State Government is absolutely essential to make sure that all States are doing the same thing on those fundamentals.

Mr. VAN DREW. If I was to ask you if Federal CDL and English proficiency standards have been consistently enforced, am I being fair when I say that some of the fatal crashes we discussed today probably could have been prevented?

Mr. SPEAR. There is absolutely no question. Your opening statement covered several crashes that we have also watched very closely. A lot of the folks that you cited in those actions, those drivers, were not able to speak English, understand English, probably should never have been driving in the first place. They were issued CDLs when they shouldn't have had them. You don't want people like that behind the wheel of a 40-ton U.S. truck.

Mr. VAN DREW. I would think. Thank you.

I am going to ask you a rapid-fire question here, and if you agree we do need to do more, if you could catch up with us and get information to me. What I am going to ask is, do you believe, in the United States of America, we need to do anything legislatively? Does Congress need to do something to make us more safe and more secure? Very briefly. I am going to ask all of you, so we have to go quickly.

Ms. de La Bruyère?

Ms. DE LA BRUYÈRE. Yes, absolutely. First, a low-hanging fruit stopping an unforced error is, with any Federal incentives or procurement, having actually enforced stringent restrictions on the ability of Chinese or Chinese-influenced entities with clear rules of what those are to receive them.

Mr. VAN DREW. I know you don't write bills, but if you could get us that information, get it to my office and also to the Committee, of what you saw, this bill gives us priorities on that.

Mr. Cole?

Mr. COLE. Yes, Mr. Chair, I do believe Congress needs to act in a few ways. First, I believe the United States Cyber Command needs additional authorities to be able to operate at the speed with which our adversaries are. I believe Congress must do more legislatively to increase our resiliency against cyberattacks.

To some degree, we have to assume that Nation-State adversaries have already compromised our infrastructure, and that means giving States the ability to more quickly respond to threats as they emerge. That could mean additional funding or clearer frameworks.

Finally, I agree with Ms. de La Bruyère that we should take a legislative approach to data sovereignty as well.

Mr. VAN DREW. Please get that to my office, both of you, as quickly as you could. Thank you.

Mr. Spear?

Mr. SPEAR. On the English language proficiency, we would advocate, for the American Trucking Associations, that Congress fully codify English language proficiency for all drivers, that all States should test for this consistently across the board. This is a safety issue.

If you are operating a vehicle, you shouldn't be pulling a U-turn on the Florida Turnpike. You should be able to understand weather signs in, say, Wyoming. You need to understand English. You need to be able to operate that equipment safely around the motoring public.

Congress needs to codify this to ensure that all 50 States abide by this and aren't just handing CDLs out carelessly to people that shouldn't be driving a 40-ton truck.

Mr. VAN DREW. Thank you. Please bring that to my office as well.

Mr. Knake?

Mr. KNAKE. I would say the most important thing, from my perspective, is to fill gaps in regulatory frameworks so that we have comprehensive ability to oversee regulation in this space.

Mr. VAN DREW. Thank you. I will yield back the rest of my time.

With that, I will yield to the Ranking Member of this Committee, Ms. Jasmine Crockett.

Ms. CROCKETT. Thank you so much, Mr. Chair.

I will point out that being a bad driver doesn't necessarily have anything to do with whether or not you can speak English. I also will point out that I have had the privilege, or maybe not so much the privilege, of driving in multiple countries, and I was not required to get another license. I was able to rent cars in other countries and drive because some things are kind of universal. Frankly, if somebody passes the test as it is laid out, then I think that this is what it is. If we need to change the test, then we need to change the test.

Nevertheless, one of the things that has become clear over the past year is that this President can be bought. If you have enough money, you can get favorable regulations from this White House. You can get pardons, you can get contracts, and you can get influence with this President, even if you have ties to a foreign government, which the Justice Department has described as—and I quote, “a significant risk to U.S. national security.”

We have already established that the Trump Administration has shown a blatant disregard for our cybersecurity. In his first month in office, the President dismantled nearly all of the DHS' advisory committees that study major cyberattacks and provide actionable recommendations to defend against those attacks.

Mr. KNAKE, what role did these advisory committees play in protecting our critical infrastructure? How does their dissolution make us less safe?

Mr. KNAKE. Thank you, Ranking Member Crockett. Absolutely, these committees were essential to establishing the mechanisms for coordinating and collaborating on cybersecurity with our industry partners. They were necessary but not sufficient. They laid the groundwork for the real-time collaborative engagement that has been emerging over the last five years.

We have gone from having just these discussions on policy and risk and threat to actually working with government agencies, with CISA, NSA, Cyber Command, and the FBI.

Ms. CROCKETT. If I am to understand you correctly, you believe that they were necessary, but you believe that they weren't even sufficient in their current form. If anything, you believe that they should have been beefed up, not deleted, correct?

Mr. KNAKE. There is absolutely a need to expand these collaborative mechanisms with industry and to make them real time and substantial. Yes.

Ms. CROCKETT. Now, I represent the State of Texas, which is the largest exporting State in the country. Texas has 32 official ports of entry that serve as critical gateways to global trade.

Mr. KNAKE, as you probably know, 80 percent of cranes at U.S. ports are manufactured by a Chinese State-owned entity, and the government has found communication devices embedded on these cranes that could be used to track port activity and enable cyber espionage. What concerns are raised when the technology used inside a critical infrastructure system is manufactured by a foreign adversary?

Mr. RASKIN. In the case of these devices, what we are talking about is an ability to both monitor and control and disrupt the infrastructure, should it be in China's interest to do so. It is an abso-

lutely critical risk that we be able to maintain our trade in the event that they feel they are compelled to use that capability.

The focus here, in my view, needs to be retrofitted at this point. We don't need to replace the steel that holds up the cranes. We are certain that is pretty strong. What we need to do is replace the electronics, rip and replace the electronics, and operate them with trusted hardware and trusted software that we know is not communicating back to China.

Ms. CROCKETT. The costs associated with operating technology needed for critical infrastructure are increasing. It doesn't help that the Trump Administration's policies are partly responsible for the cost increase. However, States are weighing the costs and availability of the technology they need to operate and maintain their critical infrastructure. There aren't domestic manufacturers for many of these necessary machines, such as cargo ships or port cranes.

Let me ask you this. We did have the CHIPS and Science Act, and my predecessor in Congress was actually the one that ushered that through. That was to make sure that we could manufacture more chips right here domestically.

It is so unfortunate because there were so many plans, and there were so many that were saying, "We are going to take advantage of this bill and pull down on these dollars," and now those plans have fallen by the wayside because of some of the terrible tariff policies that currently are taking place.

It is harming us not only economically, but it is harming us from a security standpoint. This was not fiscally responsible policy that this administration has engaged in, but it has also been very harmful to us domestically.

The last question is, so what solutions are there to mitigate the risk posed by foreign technology and infrastructure supply chains?

Mr. KNAKE. We badly need to make a government investment in the retrofitting of these technologies. The markets simply are not going to support this investment on their own, given that these are national security risks, and no risks that are necessarily going to be borne by shareholders of companies.

Ms. CROCKETT. Thank you so much for your time. I yield back.

Mr. VAN DREW. I thank the Ranking Member. I would just make one minor point that, probably, when she was driving in those foreign countries, she wasn't driving an 18-wheeler. I could probably guarantee that.

Ms. CROCKETT. How do you know?

Mr. VAN DREW. Well, I am hoping not. I couldn't even drive one. The CDL requirements are much more specific and much harder. Do you have an CDL? I don't have an CDL.

Ms. CROCKETT. I am just saying I may have.

Mr. VAN DREW. You could. You could.

Ms. CROCKETT. I got a license to carry.

[Simultaneous speaking.]

Mr. VAN DREW. Jasmine, so do I. So, do I. You never know. With that, we have—the gentleman from Texas has a UC request.

Mr. GILL. I would like to ask for unanimous consent to enter into the record this report, "The Weaponization of CISA: How a Cyber-

security Agency Colluded with Big Tech and Disinformation Partners to Censor Americans.”

Mr. VAN DREW. Without objection. I will ask the gentleman to go forward and present testimony—questions.

Mr. GILL. Thank you, Mr. Chair for holding this hearing.

In 2016, the Obama–Biden Administration issued internal guidance that weakened enforcement by discouraging roadside interviews and out-of-service penalties, effectively nullifying a core safety rule without changing the law.

Since that time, fatal truck crashes have increased, and multiple deadly incidents have involved nondomiciled or non-English-proficient drivers who should have never been licensed or allowed to operate in the first place. In many cases, they shouldn’t have even been in this country in the first place.

The Trump Administration has moved to restore the rule of law by rescinding the guidance, and even Democrat-led States such as California couldn’t hide the damage inflicted by the radical Democrats’ open-borders policies and revoked 17,000 commercial driver’s licenses given to illegal aliens.

Thank you, witnesses, for taking the time to be here.

Mr. Spear, do you consider the Obama–Biden Administration 2016 rule guidance which discouraged out-of-service enforcement for English proficiency failures to be a breakdown in regulatory control over critical transportation sector?

Mr. SPEAR. I do. That decision cost lives. Respectfully, Congresswoman Crockett, the accident that was cited in the Chair’s opening statement killed people because that driver did not understand what he was doing. An 80,000-pound vehicle is much different than a car. It does not stop on a dime. It doesn’t turn on a dime.

These are very heavy vehicles that need to have people trained and skilled to operate them, and they need to understand the language we speak. Here in America, that is English. I have lived and worked in five continents, driven in all five—Arabic, Chinese, you name it. You have to understand that country’s language to understand how to operate a vehicle. It is for the safety of those around you.

That 2016 decision by the Obama Administration took the lives of innocent people because it put people out on the road behind the wheel of an 80,000-pound vehicle that should never have been driving. We need stronger enforcement. That rule has been in the books since the 1930s. It should be consistent no matter what party you are for.

If you care about the safety of people driving in your district, then this needs to be enforced in all 50 States evenly. It is simply fundamental. There is absolutely no compromise when it comes to safety. We don’t hedge on any of that.

I want to be very clear. We need to enforce it. It needs to be done by every State. It needs to be done evenly. Yes, the language does matter.

Mr. GILL. You are exactly right. It does cost lives. It cost the life of the son of one of my constituents. A little over two years ago, eight-year-old Barron Ritchey of Pilot Point, Texas, was killed on I–35 near Hillsboro when a wheel hub and tires broke off a semi

and struck the Ritchey family's SUV as his mother drove him home from a school trip.

The non-English speaking illegal alien Martin Monreal-Alvarado had overstayed a B-1 visitor visa that expired six months prior to the incident. Further, Monreal-Alvarado was a party to RTD Carriers trucking company, an entity with an abysmal Federal Motor Carrier Safety Administration record.

The RTD Carriers employed other foreign drivers, as well, without valid work visas and sent Monreal-Alvarado on an unlawful route beyond the U.S.-Mexico-Canada Agreement commercial zone. The reality was that if even one of these issues had been policed, Barron Ritchey would still be with us today.

Mr. Spear, what can Congress do to confront unsafe carriers such as RTD from closing and reopening under a new name, reusing the same dangerous equipment and dangerous personnel?

Mr. SPEAR. Well, certainly, work with your colleagues in the Transportation Infrastructure Committee to give the Federal Motor Carrier Safety Administration at DOD the authority it needs to clean up the registry. OK? We have people come on, off, on, off. They have an accident; they come back on. They change their name.

This system is broken. The Federal oversight and ability to manage the motor carrier populace properly, safely, is broken. Secretary Duffy understands that. They are going back to the basics and enforcing the laws that you have given them. Where there are shortfalls, you all in Congress need to step up and give these agencies the power they need to have interstate commerce standards applied equally in all States.

These are just fundamentals. When you take a test in a State like California for a CDL, you need to be able to speak English. You need to be here legally. You need to have training to acquire the CDL, not some online one-day source, and you get the CDL. This has got to be enforced. I look to Congress to work with DOT to shore that up.

I can guarantee if you call over there now, they will give you a list of things that we support that will help them ensure that all States take steps forward to ensure that lives like that are not lost.

Mr. GILL. I agree, Mr. Spear. Learn English or get out of our country. Thank you for being here. I appreciate it.

Mr. VAN DREW. I thank the gentleman from Texas. That concludes today's hearing.

Ms. CROCKETT. Oh, I have got a UC. OK. "DOGE employees shared Social Security data." Court filings show employees detailed to the Social Security Administration shared sensitive data through a nonsecure server, the Justice Department disclosed. This is from *The New York Times*, January 20, 2026.

My final one is Federal review finds 44 percent of U.S. trucking schools don't comply with government rules. Nearly—this is from December 1, 2025. This is the *AP*. It says nearly 44 percent of the 16,000 truck-driving schools in the U.S. may be forced to close if they lose their students after a review by the Federal Transportation Department found they may not be complying with the government requirements. It did not say anything about languages.

Mr. VAN DREW. Without objection.

Ms. CROCKETT. OK. Now, I am good.

Mr. VAN DREW. That concludes today's hearing. We thank our witnesses for appearing before the Subcommittee today. I thank you all. You did a great job. Looking forward to the correspondence from all of you.

Without objection, all Members will have five legislative days to submit additional written questions for the witnesses or additional materials for the record.

Without objection, this hearing is adjourned.

[Whereupon, at 3:50 p.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Oversight can be found at: <https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118875>.

