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.