"Import Controls: Tools to Counter the CCP's Industrial Policy and Supply Chain Threats"

House Select Committee on the Strategic Competition
Between the United States and the Chinese Communist Party

September 16, 2026

Testimony of Peter E. Harrell

Chairman Moolenaar, Ranking Member Khanna, and distinguished Members of the Committee, thank you for giving me the opportunity to testify before you this morning.

Over the past decade, the U.S. government has steadily expanded a set of tools that I will term "national security import controls." These are measures that the government deploys to prohibit or restrict the import—and often the sale or use in the United States—of specified products, or potentially services, in order to protect U.S. national security. The government can apply national security import controls narrowly to specific products manufactured by specific firms. Or it can apply them broadly to categories of products made in specific countries. Or, as the Federal Communications Commission (FCC) has recently begun doing, to categories of products made anywhere outside the United States, with a licensing process to allow specific imports. Examples of national security import controls that many Members will be familiar with include restrictions on the use of telecommunications network equipment manufactured by the Chinese companies Huawei and ZTE, the Commerce Department's restrictions on Chinese connected vehicles, and recent actions by the FCC to bar the sale in the United States of new models of foreign-made drones, routers, robots, and power inverters.

National security import controls can be a valuable tool for preventing and reducing U.S. dependence on China (and other adversarial nations) for critical products, for reducing cybersecurity and other security risks, and for strengthening the U.S. and allied industrial base. But America's use of the tool is expanding rapidly, and the United States needs to ensure that it uses the tool both intelligently and effectively. Measures that restrict imports of a product from China (or another adversarial nation) without expanding the U.S. or allied industrial base to produce competing products risk simply cutting the United States off from useful technologies, or leaving Americans with access to those technologies only at the top end of the market. Moving too quickly to deploy national security import controls, particularly on component parts, can disrupt U.S. manufacturers, who may need time to find alternative sources of supply. Real resilience typically requires more than simply banning high-risk products, and the United States needs to embed national security import

controls within a broader set of policies that reduce U.S. vulnerabilities to Chinese coercion, espionage, and potential attacks.

My testimony today will cover five broad topics. First, I will briefly describe the history of U.S. national security import controls. Second, I will discuss the policy objectives that national security import controls can usefully serve. Third, I will offer an overview of the current regulatory landscape, in which authorities are split across multiple agencies. Fourth, I will discuss key challenges that the government needs to address in order to deploy national security import controls effectively. And fifth, I will close by offering the Committee policy recommendations regarding America's use of this toolset.

*I. History of national security import controls:*

Let me begin with some history.

America has a long history of imposing import bans or quantitative restrictions on imports during wartime. In 1917, Congress passed the Trading with the Enemy Act (TWEA) to provide the Executive Branch with broad and flexible authority to prohibit or regulate imports from Germany and its allies, alongside exports and financial transactions. TWEA is the predecessor to the International Emergency Economic Powers Act of 1977 (IEEPA), which forms the basis for most current U.S. sanctions and some current U.S. national security import controls.[1] During World War II, the Roosevelt Administration again used TWEA to restrict trade with Germany, its European allies, and Japan.

I trace the modern concept of peacetime national security import restrictions to the first decade of the Cold War. In 1954 and 1955, Congress enacted legislation that authorized the President, upon the advice of the Director of the Office of Defense Mobilization and an investigation, to "adjust the imports" of any article being imported "in such quantities as to threaten to impair the national security."[2] Today we know the successor to that 1955 law as Section 232 of the Trade Expansion Act of 1962, which most policy experts understand as the Commerce Department's national security tariff authority, and which President Trump has used to impose tariffs on a range of products including steel, aluminum, copper, lumber, polysilicon, pharmaceuticals, and, most recently, drones. But tariffs were not necessarily the statute's original purpose. The statute appears to have been designed primarily with an eye toward quantitative restrictions on imports of certain raw materials, such as the mandatory oil import quotas that President Eisenhower imposed in 1959.[3] It took a 1976

[1] Trading with the Enemy Act, ch. 106, 40 Stat. 411 (1917); International Emergency Economic Powers Act, Pub. L. No. 95-223, tit. II, 91 Stat. 1625, 1626 (1977) (codified as amended at 50 U.S.C. §§ 1701–1710).
[2] Trade Agreements Extension Act of 1955, ch. 169, § 7, 69 Stat. 162, 166. The investigative function now resides with the Secretary of Commerce. *See* 19 U.S.C. § 1862(b).
[3] Proclamation No. 3279, 24 Fed. Reg. 1781 (Mar. 12, 1959).

Supreme Court decision, *Federal Energy Administration v. Algonquin SNG, Inc.*, to establish that Section 232 authorizes monetary exactions such as license fees—the functional equivalent of tariffs—in addition to bans and quantitative restrictions. Moreover, until the last decade Presidents used Section 232 sparingly. According to the Congressional Research Service, from 1962 until 2017, the U.S. took action to directly limit imports in only a handful of cases, mostly involving petroleum, and in one case it also negotiated voluntary restraints with respect to U.S. machine tool imports.[4]

A number of factors likely explain this comparatively limited peacetime use of national security import controls until the last ten years. The United States led global technological innovation and much global manufacturing for most of the 20th century, and thus had fewer dependencies on foreign technology products than it does today. During the Cold War, American trade with the Soviet Union was limited, meaning there were few concerns about import dependencies on an adversary. Throughout the 20th century, the United States *was* concerned about the potential for foreign influence over key economic sectors and critical infrastructure, and it maintained, for example, restrictions on foreign ownership of broadcast media, civil aviation, and domestic maritime shipping. But the concern was primarily about foreign ownership and control, not imports of goods—because the United States made far more of those goods at home.

The past decade, however, has seen a rapid expansion in U.S. policymakers' focus on national security import controls. Starting in the 2010s, American policymakers in both Congress and the Executive Branch moved to restrict the use of Chinese telecommunications network equipment, particularly products made by Huawei and ZTE, in the United States. Since those initial actions, the range of products that have drawn attention has rapidly expanded to cover drones, connected vehicles, power and electrical equipment, internet routers, and robotics, among others. As I will discuss shortly, the federal government has developed a growing range of national security import bans targeting these products, with implementation authority spread across several agencies.

*II. The purposes of modern national security import controls:*

While the concept of national security import controls is not new, the types of threats against which the United States deploys them have expanded. During the Cold War, U.S. national security import controls, notably the use of Section 232, were principally designed to support the U.S. industrial base for key natural resources, such as petroleum, or certain specialty products, such as machine tools. Today, national security import controls serve at least three major sets of objectives in America's competition with China, with some import controls serving more than one:

- **First, national security import controls continue to serve as a tool to promote the U.S. (and allied) industrial base.** This is particularly important with key parts of America's

[4] Congressional Research Service, *Section 232 of the Trade Expansion Act of 1962* (updated July 2026), https://www.congress.gov/crs-product/IF13006.

industrial base, such as auto manufacturing, potentially under threat from China, and with China in a dominant manufacturing position in industries such as drones. President Trump has stated that the objective of his Section 232 tariffs is to maintain the U.S. industrial base for critical products, such as steel, although several of his uses of Section 232, such as the tariffs on lumber and wood products, have drawn criticism. But it is not just Section 232 that can support the U.S. industrial base: import bans on products such as drones can help build the U.S. industrial base by protecting upstart American manufacturers from Chinese competition, creating the economic conditions that U.S. firms need to grow.

- **Second, national security import controls can reduce the strategic leverage that China can have over the United States via its control of key supply chains.** National security import controls can force U.S. companies to reduce their dependence on China for critical products and to identify non-Chinese sources of supply. Over time, this can reduce China's ability to weaponize its control of key supply chains for geopolitical purposes.

- **Third, national security import controls can reduce domestic data security, espionage, and cybersecurity risks to key U.S. infrastructure posed by Chinese actors.** In today's connected world, a technology product imported from an adversarial nation can pose ongoing risks to U.S. national security, because the adversarial government may be able to compel the manufacturer of the product to compromise it to conduct espionage or other types of attacks in the United States. Chinese law, for example, requires Chinese organizations to "support, assist, and cooperate with" state intelligence work.[5] U.S. restrictions on the deployment of Chinese telecommunications equipment reflected concern that China could use that equipment to engage in extensive espionage in the United States.

*III. The current regulatory landscape:*

This brings me to my third topic: today's regulatory landscape. I divide the current landscape of national security import controls into four major categories:

*Section 232*:[6] Section 232 authorizes the Commerce Department to investigate whether U.S. imports of an "article" "threaten to impair the national security." If the Commerce Department determines that they do, and the President concurs, the President may "adjust" the imports of the article so that they "will not threaten to impair the national security." As I noted earlier, we tend to think of Section 232 today principally as a tariff statute, and tariffs can reduce imports in a manner that is less disruptive than an outright ban. However, the plain language of Section 232 and its history make clear that the President can also use Section 232 to prohibit imports of a wide range of goods or to

[5] National Intelligence Law of the People's Republic of China art. 7 (adopted June 27, 2017, amended Apr. 27, 2018), *available at* https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/.
[6] 19 U.S.C. § 1862, *available at* https://www.law.cornell.edu/uscode/text/19/1862.

limit their volume. The Administration's recent Section 232 polysilicon action, which establishes minimum import prices, and its Section 232 drone action, which offers tariff relief to companies that commit to U.S. production, illustrate the statute's flexibility.[7] Section 232 likely cannot be used to restrict the import of services, software, or other non-physical items, however, given that it is limited to "articles."

*The Commerce Department's "ICTS"* Rule:[8] In May 2019, President Trump signed Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," which directed the Commerce Department to establish a process to prohibit or condition transactions—including imports—involving "information and communications technology or services" designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of designated "foreign adversaries," which include China, where the transaction poses an undue risk to U.S. information and communications technology or U.S. critical infrastructure, or otherwise poses an unacceptable risk to U.S. national security.

The Commerce Department's ICTS rule can, in theory, cover a wide range of products that connect to U.S. networks. For example, both the Biden and the Trump Administrations have used the ICTS rule to restrict the sale in the United States of connected vehicles that incorporate Chinese- or Russian-linked software and hardware.[9] In June, Polestar, the electric vehicle brand controlled by China's Geely, announced that the Department had declined to authorize it to sell vehicles from model year 2027 onward and that it would wind down U.S. sales.[10] But regulatory action does not always result in a ban: The Department granted a specific authorization to Volvo, which Geely also owns, following discussions to address Volvo's governance, technology, and data security.[11] The Department has also used the ICTS rule to ban Kaspersky Lab's antivirus software, which shows that the rule reaches software as well as hardware.[12]

---

[7] Proclamation No. 11052 (Aug. 6, 2026) (polysilicon and derivatives); *see* White & Case LLP, *President Trump Orders Tariffs and Price Floors in Polysilicon Section 232 Action* (Aug. 2026), https://www.whitecase.com/insight-alert/president-trump-orders-tariffs-and-price-floors-polysilicon-section-232-action; Proclamation, *Adjusting Imports of Unmanned Aircraft Systems and Unmanned Aircraft Systems Components into the United States* (Aug. 13, 2026), https://www.whitehouse.gov/presidential-actions/2026/08/adjusting-imports-of-unmanned-aircraft-systems-and-unmanned-aircraft-systems-components-into-the-united-states/.

[8] Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 17, 2019); 15 C.F.R. pt. 791; *see also* U.S. Dep't of Com., *ICT Supply Chain*, https://www.commerce.gov/issues/ict-supply-chain.

[9] Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, 90 Fed. Reg. 5360 (Jan. 16, 2025).

[10] Press Release, Polestar, *Polestar Strengthens Its Focus on Europe Following Decision Under the U.S. Connected Vehicle Rule* (June 25, 2026), https://media.polestar.com/releases/954.

[11] Press Release, Volvo Cars, *Volvo Cars Receives a Specific Authorization in the United States Under the ICTS Connected Vehicles Rule* (May 26, 2026), https://www.volvocars.com/intl/media/press-releases/529D5DA7B9332A2C/.

[12] Final Determination: Case No. ICTS-2021-002, Kaspersky Lab, Inc., 89 Fed. Reg. 52434 (June 24, 2024).

*FCC Authorities:* Since the start of the second Trump Administration, the FCC has dramatically expanded its use of a program called the "Covered List" to restrict a range of foreign connected products in the United States.[13]

The FCC derives its authority to restrict connected products from the fact that nearly any device that emits radio frequencies—including devices that connect to Wi-Fi, Bluetooth, or cellular networks—must receive FCC equipment authorization before it can be imported, marketed, or sold in the United States. The FCC originally required authorization to ensure that such devices did not cause harmful interference, and for many devices the process is relatively routine. But in the Secure and Trusted Communications Networks Act of 2019 and the Secure Equipment Act of 2021, Congress directed the FCC to maintain a list of equipment that U.S. national security agencies determine poses an unacceptable risk to U.S. national security and to stop authorizing new models of such equipment.[14] The FCC first published the Covered List in March 2021, initially reaching equipment made by Huawei and ZTE and video surveillance and radio equipment made by three other Chinese companies, and it later added cybersecurity software made by Russia's Kaspersky Lab.

Over the past year, the FCC has substantially expanded its use of the Covered List, beginning to add entire categories of products made outside the United States, including drones and drone components, consumer-grade internet routers, power inverters, and advanced robotic devices.[15] These listings generally bar new foreign covered products from receiving FCC authorization unless the government grants an exception—for example, for foreign drones and components that the Department of War determines meet appropriate security requirements.

*Ad hoc* authorities: Beyond these three standing authorities, Presidents have used various *ad hoc* authorities to impose other national security import controls. For example, in 2024 the Biden Administration used U.S. Coast Guard authorities to direct U.S. port operators to begin addressing the cybersecurity risks posed by Chinese-made ship-to-shore cranes at U.S. ports, in response to concerns that cranes manufactured by the Chinese company ZPMC could be used for espionage or disruption.[16] The Administration also raised Section 301 tariffs on Chinese-made ship-to-shore cranes. And just last month, President Trump signed Executive Order 14421, which authorizes the Energy Department to prohibit or condition transactions involving foreign-produced equipment for

---

[13] *See* Fed. Commc'ns Comm'n, *List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist.

[14] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609); Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423.

[15] Fed. Commc'ns Comm'n, Public Notice, DA 25-1086 (Dec. 22, 2025) (drones and drone components); Fed. Commc'ns Comm'n, Public Notice, DA 26-278 (Mar. 23, 2026) (consumer-grade routers), https://www.fcc.gov/document/fcc-adds-routers-produced-foreign-countries-covered-list; Fed. Commc'ns Comm'n, Public Notice, DA 26-786 (July 28, 2026) (power inverters and advanced robotic devices), https://docs.fcc.gov/public/attachments/DA-26-786A1.pdf.

[16] U.S. Coast Guard, Notice of Availability, *Issuance of Maritime Security (MARSEC) Directive 105-4; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies*, FR Doc. No. 2024-03822 (Feb. 23, 2024), https://www.federalregister.gov/documents/2024/02/23/2024-03822/issuance-of-maritime-security-marsec-directive-105-4-cyber-risk-management-actions-for-ship-to-shore.

the U.S. bulk-power system that is linked to certain adversary countries, and even to require the isolation or replacement of such equipment already installed.[17] Like the Commerce Department's ICTS rule, Executive Order 14421 relies on IEEPA, and the President could use IEEPA to impose various other national security import controls as well. (The Supreme Court's February decision holding that IEEPA does not authorize tariffs does not appear to disturb IEEPA's use for import prohibitions of this kind.)[18]

Congress, too, is considering enacting specific national security import controls. Members of this Committee, for example, have supported legislation, the Connected Vehicle Security Act, that would permanently prohibit the import and sale of connected vehicles, software, and hardware linked to China, and the Senate Commerce Committee approved a Senate version of the bill in July.[19]

*IV. The challenges of national security import controls:*

While national security import controls can be an important tool, the United States must be clear-eyed about the challenges that can arise from their use.

The first of these is that the United States currently lacks a systematic process for determining which imports threaten U.S. national security and when a national security import control would be an appropriate response. The current process for identifying products to restrict appears to be largely *ad hoc*, driven by public policy attention focused on a discrete set of products. An *ad hoc* approach can work well enough for products where U.S. vulnerabilities seem obvious, such as drones and connected vehicles. But the United States is not well positioned to identify products whose import does pose a risk to national security but that are not well known and on which the policy community is not yet focused. An *ad hoc* approach also produces decisions that can be difficult for companies, allies, and Congress to understand or predict.

In 2024, the Commerce Department's ICTS office took a step toward addressing this gap by conducting a review, in coordination with other government agencies, of potential risks and then publishing a list of technology priorities "to respond to the most critical ICTS national security risks."[20] This document identified a number of well-known risks, such as autonomous systems and

---

[17] Exec. Order No. 14421, *Declaring a National Emergency to Secure the United States Bulk-Power System*, 91 Fed. Reg. 55995 (Aug. 31, 2026).
[18] *See Learning Resources, Inc. v. Trump*, No. 24-1287, 607 U.S. 229 (Feb. 20, 2026) (holding that IEEPA's authority to "regulate . . . importation" does not include the power to impose tariffs).
[19] Connected Vehicle Security Act, H.R. 8730, 119th Cong. (2026); Connected Vehicle Security Act of 2026, S. 4429, 119th Cong. (2026); *see* Press Release, Select Comm. on the CCP, *Moolenaar, Dingell Joint Statement on Senate Commerce Committee Passage of the Connected Vehicle Security Act* (July 22, 2026), https://chinaselectcommittee.house.gov/media/press-releases/moolenaar-dingell-joint-statement-on-senate-commerce-committee-passage-of-the-connected-vehicle-security-act.
[20] Bureau of Indus. & Sec., Off. of Info. & Commc'ns Tech. & Servs., *2024 Technology Prioritization* (2024), https://www.bis.gov/media/documents/2024-prioritization-dtd-20240516-1-20240909-revisedpdf.pdf.

robotics, but also risks that have attracted less public attention, such as satellite access points. The ICTS office, however, does not appear to have updated the list, nor has the Trump Administration published its own list of technology priorities, and the office has reportedly lost key personnel.[21] I worry that we are not making sufficient progress as a nation in identifying, to borrow former Defense Secretary Donald Rumsfeld's phrase, the "unknown unknowns": the risks posed by imports on which we are not currently focused.[22]

The second challenge is the need, in many cases, to pair national security import controls with measures to expand U.S. and allied productive capacity. We cannot simply cut off imports of risky foreign products—we also have to start building them ourselves, or in concert with allies and partners.

Take drones. In December 2025, the FCC barred the authorization of new models of foreign-made drones and drone components, and in July it proposed going further by barring continued sales of certain previously authorized foreign "military-grade" drones.[23] Last month, the President also imposed Section 232 tariffs of up to 100 percent on imported drones and drone components.[24] I have significant concerns about the risks posed by Chinese drones in the United States and China's ability to exploit them for surveillance and other purposes. But we also have to acknowledge that drones serve myriad valuable purposes in the United States, from fighting fires, to aiding law enforcement, to conducting safety inspections, to search and rescue activities. Industry estimates indicate that the United States produces fewer than 100,000 drones a year, many of them for national defense.[25] But American commercial and public-sector drone operators—energy companies, police departments, Hollywood cinematographers, construction companies, and the like—have registered more than one million drones with the Federal Aviation Administration (FAA), with 126,000 commercial operators registering equipment in 2025 alone.[26] The FAA estimates that hobbyists fly roughly 1.6 million more.[27] The FAA also reports that drone imports fell by roughly three-quarters in 2025 while the average price of imported drones more than doubled, and that most U.S. drone manufacturers still rely on Chinese batteries, motors, flight controllers, and circuit

---

[21] Justin Sherman, *Another Misstep in U.S.-China Tech Security Policy*, Lawfare (Feb. 3, 2026), https://www.lawfaremedia.org/article/another-misstep-in-u.s.-china-tech-security-policy.
[22] U.S. Dep't of Def., News Transcript, *DoD News Briefing—Secretary Rumsfeld and Gen. Myers* (Feb. 12, 2002).
[23] Fed. Commc'ns Comm'n, Fact Sheet, *FCC Updates Covered List to Include Foreign UAS and UAS Critical Components on Going Forward Basis* (Dec. 22, 2025), https://docs.fcc.gov/public/attachments/DOC-416839A1.pdf; Fed. Commc'ns Comm'n, Fact Sheet, *FCC Takes Action to Secure the Drone Supply Chain* (July 21, 2026), https://docs.fcc.gov/public/attachments/DOC-423277A1.pdf.
[24] Proclamation, *Adjusting Imports of Unmanned Aircraft Systems and Unmanned Aircraft Systems Components into the United States* (Aug. 13, 2026), https://www.whitehouse.gov/presidential-actions/2026/08/adjusting-imports-of-unmanned-aircraft-systems-and-unmanned-aircraft-systems-components-into-the-united-states/.
[25] N.Y. Times (July 13, 2025), https://www.nytimes.com/2025/07/13/business/drones-us-military-manufacturing-lags.html; *see also Drones Are Changing Warfare. The US Is Trying to Catch Up.*, Christian Sci. Monitor (Dec. 1, 2025), https://www.csmonitor.com/USA/Military/2025/1201/drones-hegseth-military-warfare (reporting that the United States produces fewer than 100,000 drones a year, about half for military purposes).
[26] Fed. Aviation Admin., *Compendium to FAA Aerospace Forecast 2026–2046: Emerging Aviation Entrants* 11–14 (2026), https://www.faa.gov/data_research/aviation/aerospace_forecasts/uas-compendium.pdf.
[27] *Id.* at 8–9.

boards.[28] If we cut off imports without drastically expanding the U.S. and allied drone industrial base, we will reduce China-related drone risks but at the cost of having less access to drones in the United States, including for important economic and safety activities.

Now, an import ban itself can be an important part of the industrial policy needed to expand U.S. or allied capacity. It is hard for U.S. drone makers to attract capital and scale up if they face relentless price competition from Chinese competitors. The FCC reports that more than $4 billion has flowed to U.S.-based drone and related production companies since its December action.[29] The Trump Administration has also promoted a "drone dominance" agenda, including a $1.1 billion Pentagon program to buy low-cost, American-made drones at scale.[30] Given the size of the gap between U.S. demand and U.S. production, however, it is clear that more needs to be done.

A third challenge with national security import controls is to ensure that the United States does not fall into the trap of assuming that banning imports of foreign products is sufficient to eliminate national security risks.

The U.S. experience with Huawei and ZTE telecommunications equipment illustrates this point. Congress restricted federal procurement of Huawei and ZTE equipment in 2018, and in the Secure and Trusted Communications Networks Act of 2019 it directed the FCC to create the Covered List, on which Huawei and ZTE were among the first five companies placed in March 2021.[31] Congress also funded a "rip and replace" program to help telecommunications carriers, many of them smaller rural carriers, replace older Huawei and ZTE equipment with trusted alternatives (although the program was so underfunded for several years that the FCC could initially cover only about 40 percent of approved costs).[32]

But while the import ban and related efforts closed off one avenue for Chinese espionage—Huawei and ZTE network gear deployed in the United States—policymakers and the telecommunications industry paid far too little attention to another avenue: sophisticated Chinese hackers simply breaking into Western-made network equipment. According to the U.S. government, Chinese state-

---

[28] *Id.* at 27–30.
[29] Fed. Commc'ns Comm'n, Fact Sheet, *FCC Takes Action to Secure the Drone Supply Chain* (July 21, 2026), https://docs.fcc.gov/public/attachments/DOC-423277A1.pdf.
[30] Exec. Order No. 14307, *Unleashing American Drone Dominance*, 90 Fed. Reg. 24727 (June 11, 2025); Memorandum from the Sec'y of Def., *Unleashing U.S. Military Drone Dominance* (July 10, 2025); U.S. Dep't of War, *Drone Dominance Program Receives First Order, Gauntlet II Gets Underway*, DoD News (June 17, 2026); Press Release, U.S. Dep't of War, *War Department Announces Vendors Invited to Compete in Phase I of the Drone Dominance Program*, https://www.war.gov/News/Releases/Release/Article/4396462/war-department-announces-vendors-invited-to-compete-in-phase-i-of-the-drone-dom/.
[31] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636, 1917 (2018); Fed. Commc'ns Comm'n, *List of Equipment and Services Covered by Section 2 of the Secure Networks Act*, https://www.fcc.gov/supplychain/coveredlist (listing dates of inclusion).
[32] Cong. Rsch. Serv., R48534, *Advanced Wireless Services (AWS-3) Spectrum: Issues for Congress* (2026), https://www.congress.gov/crs-product/R48534; *FCC Repays Big Treasury Loan Following Auction Success*, Radio & Television Bus. Rep. (Sept. 2026), https://rbr.com/fcc-repays-big-treasury-loan-following-auction-success/ (reporting that the FCC initially allocated only about 39.5 percent of approved costs).

sponsored hackers, in a campaign widely known as "Salt Typhoon," exploited vulnerabilities in routers and other network equipment made by U.S. and other Western companies, including Cisco, to penetrate deep into U.S. telecommunications networks.[33] The hackers even copied information subject to court-ordered law enforcement requests, such as wiretaps.[34] A separate Chinese campaign, known as "Volt Typhoon," used hundreds of hijacked, outdated U.S.-brand routers to conceal efforts to pre-position inside U.S. critical infrastructure.[35]

On the one hand, the Salt Typhoon and Volt Typhoon campaigns vindicate the U.S. decision to ban Huawei and ZTE equipment: clearly, China wanted to infiltrate U.S. telecommunications infrastructure, and Huawei and ZTE equipment presumably would have given it an easy avenue to do so. On the other hand, the bans did not prevent profoundly concerning levels of Chinese espionage against Americans via American telecommunications networks.

We need to be careful not to let this happen again. For example, I generally support measures to ban the deployment of Chinese connected vehicles in the United States, such as the ban in the Connected Vehicle Security Act that Congress is currently considering. But if we focus only on banning Chinese connected and autonomous vehicles, without making sure that Waymo, Tesla, and other U.S. autonomous vehicle companies harden their vehicles and systems against Chinese attacks, China may simply find a way to conduct mobile surveillance and potentially disrupt U.S. transportation by hacking into those companies' systems. The same is true of the power grid: Executive Order 14421's restrictions on adversary-linked equipment will need to be paired with serious cybersecurity requirements for the trusted equipment that replaces it.

A fourth challenge is the need to work with allies and partners. There are two reasons to do so.

First, we have a national security interest in our allies not being dependent on China and other adversaries for key products. For example, sensitive U.S. military and corporate data travel across telecommunications networks in the European Union, given the U.S. military bases in Europe, the major operations that many U.S. companies have in Europe, and the major operations that many European companies have in the United States. We thus have an interest in Europe reducing its use of Chinese telecommunications network equipment as we work to reduce our own.

---

[33] Cybersecurity & Infrastructure Sec. Agency et al., Joint Cybersecurity Advisory AA25-239A, *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System* (Aug. 27, 2025), https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[34] Press Release, Fed. Bureau of Investigation & Cybersecurity & Infrastructure Sec. Agency, *Joint Statement from FBI and CISA on the People's Republic of China Targeting of Commercial Telecommunications Infrastructure* (Nov. 13, 2024), https://www.fbi.gov/news/press-releases/joint-statement-from-fbi-and-cisa-on-the-peoples-republic-of-china-targeting-of-commercial-telecommunications-infrastructure.

[35] Press Release, U.S. Dep't of Just., *U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure* (Jan. 31, 2024), https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical.

Second, working with allies and partners is an important part of industrial policy. Manufacturing at the scale needed to compete with China will in many cases require a larger market than the United States alone, and combining our markets, while protecting them from adversarial products, will increase innovation and economic efficiency.

Working with allies and partners means practical coordination, not necessarily identical steps. But it also means designing our own controls so that they do not shut out the very allied suppliers we need. An example from earlier this year illustrates both points. In May, the European Commission began restricting EU funding for energy projects that use inverters from high-risk countries, including China, citing cybersecurity risks.[36] In July, the FCC barred new models of foreign-produced power inverters from the U.S. market.[37] The two actions used different legal authorities and had different scopes, but both leveraged existing authorities to address the same underlying threat—and in that respect they offer a model for how cooperation can work in practice.

Finally, especially when it comes to national security import restrictions on certain types of *software*, there is not a clear-cut legal authority to enact a national security import control. Take an example that I know is on the minds of many Members of this Committee: open-weight Chinese AI models, such as those released by DeepSeek, Alibaba (Qwen), Zhipu AI (Z.ai), and Moonshot AI (Kimi), which publish their model weights online, free for anyone to download. There is not currently a U.S. law that clearly authorizes the U.S. government to restrict Americans from simply downloading and using such models. IEEPA contains an exception for "informational materials" that a federal court relied upon in 2020 to block the first Trump Administration's restrictions on TikTok, and restrictions on the distribution of software can raise First Amendment questions, as the parallel litigation over WeChat showed.[38] Congress ultimately addressed TikTok through targeted legislation.[39] In today's technologically enabled world, where software can pose as serious a security threat as devices, we need to make sure our legal regime provides the authority to address the full range of threats.

*V. Recommendations:*

Against that backdrop, let me close by offering five policy recommendations for the Committee's consideration.

---

[36] Tristan Rayner, *EU Funding Ban on High-Risk Inverters, Including Chinese Suppliers, Extends to BESS*, PV Magazine (May 4, 2026), https://www.pv-magazine.com/2026/05/04/eu-funding-ban-on-high-risk-inverters-including-chinese-suppliers-extends-to-bess/; *see also* Le Monde (May 4, 2026), https://www.lemonde.fr/en/international/article/2026/05/04/eu-blocks-funding-for-certain-chinese-solar-tech_6753117_4.html.

[37] Fed. Commc'ns Comm'n, Public Notice, DA 26-786 (July 28, 2026), https://docs.fcc.gov/public/attachments/DA-26-786A1.pdf.

[38] 50 U.S.C. § 1702(b)(3); *see TikTok Inc. v. Trump*, 490 F. Supp. 3d 73 (D.D.C. 2020); *Marland v. Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020); *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912 (N.D. Cal. 2020).

[39] Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 895, 955 (2024); *see TikTok Inc. v. Garland*, 145 S. Ct. 57 (2025) (per curiam).

*First, establish a systematic and transparent process for identifying import risks and imposing national security import controls.*

As I discussed earlier, the U.S. currently has an *ad hoc* approach to identifying what imports threaten U.S. national security and when national security import controls should be deployed. Having served in government, I understand jurisdictional realities and do not necessarily object to different agencies having different authorities to impose national security import controls. But we do need a comprehensive risk assessment, a coherent process for identifying priorities, and a process for action. Congress should require the Executive Branch to conduct and publish an annual interagency assessment of priority products that the government would then consider for action, potentially modeled after the ICTS office's 2024 technology priorities list. The Executive Branch should also be required to publish more information about why it thinks imports or use of a particular product poses a risk to U.S. national security—much as the government currently does with Section 232—and how it assesses when to mitigate risks rather than impose an outright national security import restriction.

*Second, give the United States a durable and comprehensive legal regime.*

Several existing national security import controls, including the ICTS rule and the new restrictions on power grid equipment, exist pursuant to the 1977 emergency powers statute, IEEPA. But the risks that these programs are designed to address are not emergencies—they are structural and ongoing risks—and IEEPA is not a statute purpose-built to address them. Congress should codify the ICTS program in statute, with clear standards for use, and consider broader legislation that would codify other national security import controls as well.

Congress should also close the gap for software. Congress could authorize the Executive Branch, subject to appropriate findings, to restrict the use of specified adversary AI models and other software by critical infrastructure operators and others in the private sector, and to restrict the commercial hosting and deployment of such models by U.S. companies.

*Third, pair national security import controls with industrial policy.*

As I discussed, import controls should generally be paired with industrial policy measures to ensure that the U.S., and its allies, can in fact develop alternative suppliers to replace high-risk products from our adversaries and competitors. Many tools for these programs already exist: federal procurement commitments like the Pentagon's Drone Dominance Program, Office of Strategic Capital lending, Defense Production Act Title III investments, and federal grant programs that can help state and local agencies purchase trusted equipment. The government needs to make sure that it is consistently deploying these tools alongside national security import controls. And the tools need to reach upstream components as well as downstream finished products: an American drone that

depends on Chinese sensors and batteries, for example, continues to pose risks and give China leverage.

*Fourth, embed each import control in a broader strategy that actually addresses the underlying risk.*

A national security import control should be just one element of a plan to mitigate the risk that prompted it, not a substitute for a plan. Agencies responsible for imposing national security import controls should identify other avenues that an adversary could exploit to achieve the same objective that the import control is designed to prevent, such as cyberattacks on trusted equipment and remote access by service providers. In practice, this will mean pairing import restrictions on adversary connected vehicles with cybersecurity standards for U.S. and allied connected vehicles; pairing restrictions on adversary grid equipment with serious cybersecurity requirements for the equipment that replaces it; and ensuring that the lessons of Salt Typhoon translate into enforceable security obligations for telecommunications carriers. Congress should require agencies to report on these measures and to develop periodic assessments of whether import controls are achieving their objectives.

*Finally, take an allied approach by default.*

The U.S. needs to make sure that it is working with allies and partners by default. We should be willing to accept products made by our allies—as long as they meet appropriate cybersecurity or other standards. The United States should coordinate risk assessments, priority products and sectors, and trusted-vendor lists with allies such as the European Union, Japan, South Korea, the U.K., Australia, and other partners. And it should explore joint procurement and co-investments to build a trusted allied market at the scale needed to compete with China. Our allies' security is bound up with our own, and the scale of a combined market is one of the most important advantages we have.

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

*Panelist note:* Harrell thanks his Georgetown research assistant, Dayle Foster, for her assistance with the research. In addition to the assistance provided by Ms. Foster, Harrell used generative AI in his research for this testimony, to assist with formatting footnotes, and to copy-edit the document. The testimony itself represents Harrell's ideas and writing.