February 1, 2024

Statement of Hon. Nazak Nikakhtar*

Partner, International Trade, National Security Practice Chair, Wiley Rein LLP
Former Assistant Secretary for Industry & Analysis, Under Secretary for Industry & Security
U.S. Department of Commerce

Testimony Before the United States-China Economic and Security Review Commission*

Current and Emerging Technologies in U.S.-China Economic and National Security Competition

I. INTRODUCTION

Co-Chair Commissioner Michael Wessel and Co-Chair Commissioner Jacob Helberg, and all Commissioners, thank you for the opportunity to speak about the threats posed by the People's Republic of China and the Chinese Communist Party ("CCP"), specifically the presence of Chinese-manufactured hardware and software in the information technology networks of sensitive Government and commercial systems in the United States. My focus today is on potential hardware vulnerabilities in Chinese information technology products.

My name is Nazak Nikakhtar, and it is an honor to appear before you today. I am an international trade and national security attorney, and I chair the national security practice at the Washington, DC, law firm of Wiley Rein LLP. I am also a trade and industry economist, a former Georgetown University adjunct law professor, and I recently completed my second tour in the U.S. Government. Twenty years ago, I began my career as an analyst at the U.S. Department of Commerce's Bureau of Industry and Security and subsequently at the International Trade Administration, where my colleagues and I witnessed, from the frontlines, the United States' steady erosion of its domestic industrial base. Beginning in the early 2000s, America rapidly transferred production capacity and technology to China, and we now find ourselves relying on Chinese components to power our most sensitive electronic devices – from commercial items to defense articles. And because China is an adversary, it is leveraging our supply chain dependence against us. The Chinese hardware we use contain backdoors that allow critical systems to be infiltrated by malicious software. And China has a bigger hacking program than every other country in the world combined. The system failure vulnerabilities at America currently faces nationwide are beyond alarming, they are likely catastrophic.

**The views and opinions expressed in this testimony are mine only and do not present the views of Wiley Rein LLP or any of the firm's clients.*

In 2004, I helped institute Commerce's China/Non-Market Economy Office where we warned the broader U.S. Government about such supply risks. Then, for several years thereafter, I audited numerous foreign (including Chinese) companies and their affiliates for the Commerce Department and witnessed firsthand China's efforts to decimate our most critical production capabilities to gain the upper hand. In 2018, I returned to the Commerce Department to serve as Assistant Secretary for Industry & Analysis and, in 2019, I simultaneously served, performing the non-exclusive functions and duties, as the Under Secretary for the Bureau of Industry and Security. My time at Commerce, from 2018 through 2021, marked the first time in modern U.S. history that the Executive Branch tackled critical supply chain vulnerabilities. Many of those efforts were spearheaded by my offices from 2018 to 2020. We rolled out the United States' whole-of-government semiconductor strategy in 2018, and, in 2019, we tackled head-on the risks arising from technology transfer to China. We were the first advocates for a meaningful American industrial base strategy to reshore critical capabilities and grow the American workforce. And, in 2019 and 2020, we rolled out innovative legal strategies to prevent malicious Chinese hardware and software from infiltrating America's infrastructure and undermining our national security.

Today, my work to protect national security continues in the private sector. Altogether, I have been working to strengthen the U.S. commercial and defense industrial base for the past 20+ years. It is from all of these vantage points that I offer my testimony and observations today.

II. CHINESE LAWS CREATE THE THREAT TO U.S. NATIONAL AND ECONOMIC SECURITY

First and foremost, context is important. China and other foreign adversaries pose significant national security threats to the United States. China, in particular, is undermining the peace and stability of the world order by threatening to harm the United States and its allies, and it is weaponizing its supply chains, intellectual property ("IP"), and technologies against the rest of the world. And I want to be clear that this is a fact, not conjecture - it is a matter of Chinese law. The CCP compels Chinese companies, including American firms in China forced to form joint ventures, to serve the country's national security interests through a variety of legal measures. The country's Civil-Military Fusion strategy imposes the CCP's ultimate control over all Chinese corporations through a range of national security laws. These laws demand that Chinese entities cooperate with the People's Liberation Army ("PLA") to advance the military strength and ambitions of the CCP for global power.

All Chinese entities, even those enterprises that still remain ostensibly private and civilian, are legally obligated to serve the state and the leadership of the central government such that Chinese entities have limited autonomy over their business decisions. The CCP's routine installation of CCP officials inside private firms – including American businesses in China – ensures compliance with the party's mandates. The Chinese nationwide credit rating system for all corporations operating with in China further requires that companies follow CCP laws or risk losing business opportunities. CCP laws further require that sensitive data (including personal data and intelligence data) and proprietary technical information, including IP, be transferred to the CCP whenever requested. The laws also prohibit all companies in China from complying with the laws of other jurisdictions, including U.S. national security sanctions and export control laws. The

objective of the CCP's laws is to coerce the sizeable Chinese commercial sector to align with the CCP's interests and to transfer technological innovations and information to the PLA to augment its military power.

The reality is that Chinese entities operate in a highly-controlled government- and military-driven ecosystem that is designed to advance the country's military capabilities, intelligence and surveillance operations, and national security apparatus. The legal framework through which the CCP forces entities to contribute to the modernization and expansion of the CCP's capabilities continues to expand rapidly through the promulgation of far-reaching laws and policies. The CCP's legal mandates direct corporate practices in China such that our hardware supply chain dependence poses a significant threat to the national security and economy of the United States. A summary of some of the most relevant CCP laws is provided in **Appendix 1**.

III. AMERICA'S SUPPLY CHAIN VULNERABILITIES ARE SIGNIFICANT

Today there are over 700 items – raw materials, semifinished goods, and finished goods – that are essential to U.S. national security, and the majority of these supply chains are concentrated or maintained exclusively in China. Much of these supply chains include critical hardware (as well as the raw materials necessary to manufacture the hardware) – such as semiconductors, microprocessors, and electronic computing systems – with backdoor capabilities permitting software enabled security risks. Their use in commercial electronic devices, such as personal computers and handsets, pose significant surveillance risks to users. And these devices' connections to critical U.S. infrastructure poses substantial dangers through the transfer of software from, e.g., personal computing devices, to modems or hardware modules in telecommunications towers, for example.

While it is impossible to list all the places where Chinese hardware exist and the resulting threats to the U.S. infrastructure, the illustrations in this paper are intended to provide examples of current vulnerabilities. To emphasize, however, the extent of Chinese hardware penetration in U.S. systems is far greater. As FBI Director Wray testified to Congress:

> China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. If or when China decides the time has come to strike, they're not focused solely on political or military targets. We can see from where they position themselves, across civilian infrastructure, that low blows aren't just a possibility in the event of a conflict. Low blows against civilians are part of China's plan.[1]

Obviously, the United States needs to develop and implement viable national strategy to protect its essential security interests. It does not have one yet, and time is running out.

[1] FBI, News, Director Wray's Remarks to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Jan. 31, 2024).

A. Telecommunications Infrastructure and Personal Devices

It is well documented that Chinese hardware has infiltrated telecommunications networks across the country and poses a direct threat to U.S. national security and American privacy. Yet is counterintuitive that the U.S. Government has, to date, done nothing meaningful about it.

Congress and the Executive Branch are well aware of and have been working to address hardware vulnerabilities in the telecommunications sector for several years. Senators Markey and Wyden wrote to the Federal Communications Commission ("FCC") in 2021 regarding potential national security risks posed by foreign companies that manage and service U.S. wireless phone networks.[2] It is very common for the U.S. wireless industry to outsource the installation and administration of networking technology to managed service providers, some of which are foreign service providers subject to the jurisdiction of foreign countries of concern.[3] For example, the U.S. Federal Bureau of Investigation found in 2022 that Chinese company Huawei Technologies Co., Ltd.'s equipment was widespread in cell towers in close proximity to sensitive military bases.[4] The FBI recognized that Huawei equipment has the ability to intercept commercial cell traffic, access restricted U.S. military airwaves, and disrupt U.S. strategic command communications, potentially providing a window into the U.S. nuclear arsenal.[5] Given this risk, the FCC designated Huawei to its "Covered Equipment or Services" List in 2021 and it issued a rule in 2022 banning American carriers from using federal subsidies to procure equipment from Huawei and other entities on the Covered List.[6] Subsequently, in February 2023, the FCC prohibited Covered Equipment from obtaining *new* equipment authorizations. The new prohibition did not apply to any equipment with *prior* authorization, moreover, meaning that much of Huawei equipment still remains in telecommunications networks including infrastructure close to sensitive military installations.[7]

In 2019, following the U.S. Department of Commerce's decision to place Huawei on the Entity List,[8] Congress allocated $1.9 billion through the Secure and Trusted Communications Network Act to reimburse small cellular and broadband providers to "rip and replace" Huawei and ZTE

---

[2] Letter from Off. of Ron Wyden, U.S. Senator, to Jessica Rosenworcel, Acting Chairwoman, Federal Communications Commission (Oct. 20, 2021), *available at* https://docs.fcc.gov/public/attachments/DOC-392396A1.pdf.

[3] *Id.*

[4] Katie Bo Lillis, *CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications*, CNN (July 25, 2022), *available at* https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

[5] *Id.*

[6] Brian Fung, *US regulators rule that China's Huawei and ZTE threaten national security*, CNN Business (Nov. 22, 2019), *available at* https://www.cnn.com/2019/11/22/tech/fcc-huawei-zte/index.html.

[7] Federal Communications Commission, Prohibition on Authorization of "Covered" Equipment (last updated Feb. 6, 2023), *available at* https://www.fcc.gov/laboratory-division/equipment-authorization-approval-guide/equipment-authorization-system.

[8] *Addition of Entities to the Entity List*, 84 Fed. Reg. 22,961 (Dep't Commerce May 21, 2019).

equipment on their networks.[9] To date, the FCC has been confronting repeated problems with the delay-ridden rip and replace program,[10] including the fact that the cost of this rip and replace effort is more than double the estimated $1.9 billion.[11] Absent additional appropriations, the FCC is only able to reimburse companies for a fraction of their rip and replace costs.[12] As of May 2023, 15% of projects approved for rip and replace have not commenced at all, continuing to put sensitive U.S. telecommunications in peril of interception by the CCP.[13]

The U.S. Department of Commerce is additionally probing whether, and the extent to which, Huawei gear is able to intercept communications from nearby missile silos.[14] Huawei hardware placed near U.S. military installations across the United States may already be obtaining sensitive information about the sites, not only about the number of people on duty in buildings and when equipment is online and offline, but also through the interception of actual missile communications from the silos. The risk also exists that Huawei hardware can facilitate access to the computer and telecommunications networks that are operating the silos.[15]

Recently, the House Select Committee on the Chinese Communist Party identified additional risks arising from hardware modules in internet of things ("IoT") devices manufactured by Chinese entities Quectel and Fibocom. These companies own a significant market share of IoT modules globally,[16] and are in part owned by the CCP:[17]

> Quectel is an IoT service provider, and it is the world's largest supplier of IoT modules. The company supplies cellular modules, WiFi/GNSS modules, and IoT antennas. Products are mainly used in the fields of wireless payment, vehicle transportation, smart energy, smart city, intelligent security, wireless gateway, industrial applications, medical health, and agricultural environment. The company, which was founded in Shanghai in 2010, was listed on the Shanghai Stock Exchange in 2019. Over 60% of Quectel's shares are public free float. At least 3.6% up to 6.2% of Quectel is owned by the CCP.[18]

---

9 U.S. Senate Committee on Commerce, Science, and Transportation, *Press Release: President Signs Rip and Replace Bill Into Law* (Mar. 12, 2020), *available at* https://www.commerce.senate.gov/2020/3/president-signs-rip-and-replace-bill-into-law.

10 *See* Jared Foretek, *FCC's 'Rip And Replace' Delays Upset Rural Providers*, Law360 (Nov. 16, 2023), *available at* https://www.law360.com/articles/1767711/fcc-s-rip-and-replace-delays-upset-rural-providers.

11 *See* Katie Bo Lillis, *supra* note 3.

12 *Id.*

13 Makena Kelly, *Congress called Huawei a national security risk — it's still in US networks*, The Verge (May 15, 2023), *available at* https://www.theverge.com/23721573/huawei-zte-rip-and-replace-china-telecom-carriers-fcc.

14 *See* Katie Bo Lillis, *supra* note 3.

15 Alexandra Alper, *Exclusive: U.S. probes China's Huawei over equipment near missile silos*, Reuters (July 21, 2022), *available at* https://www.reuters.com/world/us/exclusive-us-probes-chinas-huawei-over-equipment-near-missile-silos-2022-07-21/.

16 Alexi Drew, *Chinese technology in the 'Internet of Things' poses a new threat to the west*, Financial Times (Aug. 10, 2022), *available at* https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117.

17 WireScreen, The Leading China Business Intelligence Platform, *available at* https://www.wirescreen.ai/.

18 *Id.*

> Fibocom is a leading global provider of IoT wireless solutions and wireless communication modules. In 2017, Fibocom become the first listed wireless module provider in China. Fibocom provides modules to Huawei, Hikvision, and SZ DJI Technology Co., Ltd. or Shenzhen DJI Sciences and Technologies Ltd. ("DJI"), all three of which have come under scrutiny from the U.S. government. At least 5.4% up to 9.9% of Fibocom is owned by the Chinese government. [19]

In September 2023, FCC Chairwoman Rosenworcel asked U.S. Government agencies to consider declaring that Quectel and Fibocom pose unacceptable national security risks.[20] Their modules are used throughout the United States by U.S. and foreign companies, and Quectel has nearly exclusive market share in the United States, as there are millions of Quectel modules in the telecommunications infrastructure and in smart devices across the country.[21] The letter to the FCC also details that Quectel and Fibocom contribute to China's defense industrial base by supplying Huawei and numerous firms designated by the U.S. Department of Defense ("DOD") as PLA affiliates and firms listed on the FCC's Covered List.[22]

TikTok is another important example of a major threat. It is well established that the Chinese government has been spying on Americans through the TikTok personal device application ("app"), controlled by Chinese parent company ByteDance. Beyond surveillance capabilities, the TikTok app has the ability to transfer malicious software to the hardware contained in devices in close proximity to it (e.g., from personal handsets to U.S. Government computers) and to the hardware installed in telecommunications infrastructure (e.g., modems and modules). In January 2023, the U.S. military banned TikTok from government devices after the DOD labeled it a security risk.[23] Approximately 34 states have already banned employees from using the app on government devices,[24] and in February 2023, the Biden Administration prohibited federal agencies from installing the app on their Government devices. There is also growing international consensus about the risks arising from the TikTok app. Looking abroad, India took the lead in banning the platform in 2020. Other countries and government bodies — including the United Kingdom, Australia, Canada, the executive arm of the European Union, France, and New Zealand's parliament — have similarly decided to ban the app from government devices as well.[25] Yet

---

19 *Id.*

20 David Shepardson, *US FCC chair says China's Quectel, Fibocom may pose national security risks*, Reuters (Sept. 6, 2023), *available at* https://www.reuters.com/technology/us-fcc-chair-asks-agencies-consider-restrictions-quectel-fibocom-2023-09-06/.

21 *Id.*

22 *Id.*

23 Brandi Vincent, *Pentagon issues rule to ban TikTok on all DOD-connected devices, including for contractors*, DefenseScoop (June 2, 2023), *available at* https://defensescoop.com/2023/06/02/pentagon-proposes-rule-to-ban-tiktok-on-all-dod-connected-devices-including-for-contractors/.

24 Brian Fung and Christopher Hickey, *TikTok access from government devices now restricted in more than half of US states*, CNN Business (Jan. 16, 2023), *available at* https://www.cnn.com/2023/01/16/tech/tiktok-state-restrictions/index.html.

25 Sapna Maheshwari and Amanda Holpuch, *Why Countries Are Trying to Ban TikTok*, New York Times (Dec. 12, 2023), *available at* https://www.nytimes.com/article/tiktok-ban.html.

despite the widespread acknowledgement of the risks posed by TikTok, the U.S. federal government has done little more to protect Americans from this risk.

Finally, the RISC-V open source chip design architecture is creating significant vulnerabilities in devices in which they are installed. The architecture is heavily leveraged by Chinese (and Russian) companies to undermine U.S. technological advantages in telecommunications related systems such as artificial intelligence ("AI"), autonomous systems, high-performance computers, and semiconductors. This is because the open-source nature of RISC-V's designs provide adversaries with the architectural designs and information to access and embed cybersecurity vulnerabilities at the chip design phase creating significant openings for exploitation. Chinese companies have become major contributors to RISC-V, and the CCP's national champions Huawei Technologies, ZTE Corp, and Alibaba Group Holding Ltd. are all members of RISC-V International, the global non-profit standards home of the open standard RISC-V Instruction Set Architecture. In 2022, 10 billion RISC-V chips were produced globally, of which half were made in China. Current U.S. regulations do not capture this technology, once again giving rise to major national security risks.

B. Military Materiel and Defense Networks

The degree to which U.S. military platforms depend on Chinese hardware is alarming. It is estimated that approximately 41% of DOD weapon systems and infrastructure supply chains rely on Chinese semiconductors.[26] U.S. Navy vessels, in particular, are utilizing thousands of Chinese semiconductors in critical naval ships with the U.S.'s carrier fleet, the workhorse of the U.S. Navy[27] and the heart of USINDOPACOM's strategic capabilities,[28] utilizing over 5,000 Chinese semiconductors per carrier.[29] Additionally, the U.S. Navy uses Chinese hardware in a variety of other essential naval military platforms, including the F/A 18 aircraft, the F/A 18 Growler, and the Navy's air-launched armament, including JASSM, JDAM, LRASM, and Tomahawk cruise missiles.[30]

The DOD's information technology ("IT") ecosystem is severely vulnerable according to a 2019 DOD Inspector General report, which found that at least $32.8 million of commercial off-the-shelf IT items procured by DOD officials had known cybersecurity vulnerabilities in FY 2018 alone.[31] This was a limited-scope study focused on Army and Air Force Government Purchase Card holders. The result was the purchases of high-risk electronic items, such as Lenovo computers,

---

[26] Jeffrey Nadaner and Tara Dougherty, *Numbers Matter: Defense Acquisition, U.S. Production Capacity, and Deterring China*, Govini, *available at* https://govini.com/research/numbers-matter-2024/ ("Govini Report").

[27] U.S. Navy, Aircraft Carriers – CVN (Nov. 12, 2021), *available at* https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2169795/aircraft-carriers-cvn/.

[28] U.S. Navy, Commander, U.S. 7th Fleet, The United States Seventh Fleet, *available at* https://www.c7f.navy.mil/About-Us/Facts-Sheet/.

[29] Govini Report.

[30] Govini Report.

[31] U.S. Dep't of Defense, Inspector General, *(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items* at i, *available at* https://www.oversight.gov/report/DoD/Audit-DoD%E2%80%99s-Management-Cybersecurity-Risks-Government-Purchase-Card-Purchases-Commercial.

which the DOD believes can severely compromise electronic defense platforms and classified information systems.

Chinese companies identified by the DOD as being high-risk companies have not been excluded from the domestic supply chain. In 1999, the National Defense Authorization Act ("NDAA") mandated that the DOD identify Communist Chinese military companies ("CCMC") operating directly or indirectly in the United States or in any of its territories or possessions pursuant to section 1237.[32] The Department issued its first CCMC list 20 years later in 2020, and designated dozens of Chinese companies to the list over the course of several subsequent months. Immediately thereafter, section 1260H of the 2021 NDAA became law and expanded the definition of Chinese military companies in order to enhance the DOD's ability to keep pace with the CCP's and the PLA's expanding control over the Chinese commercial sector.[33] The DOD then sunsetted the 1237 list and, despite having a new legal authority to designate a greater number of PLA companies to its list, the Pentagon opted to designate a smaller subset of companies to its new 1260H list.[34] The reason for this is unclear.

The 1260H designation has very limited legal implications, namely for U.S. Government contractors and other companies participating in the U.S. Government's supply chain. The Federal Acquisition Regulations ("FAR") prohibit U.S. Government agencies from "procuring or obtaining" "any equipment, system, or service" that utilizes "covered telecommunications equipment or services" for certain critical technology or a "substantial or essential component of any system."[35] While Congress in 2019 identified five Chinese companies as being subject to the FAR prohibitions, the statute and implementing regulations can apply to any other company "that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a foreign country.[36] Further, the DOD's supplement to the FAR (the Defense Federal Acquisition Regulation Supplement, "DFARS") prohibits the acquisition of items covered by the United States Munitions List from a 1260H company.[37] Moreover, Section 514 of the Consolidated Appropriations Act for 2018 specifies that for "high-impact or moderate-impact" information systems, agencies must review the "supply chain risk,"

---

[32] *Strom Thurmond National Defense Authorization Act for Fiscal Year 1999*, Public Law 105-261 (as amended by section 1233 of Public Law 106-398 and section 1222 of Public Law 108-375), U.S. Congress (Oct. 17, 1998), *available at* https://www.govinfo.gov/link/plaw/105/public/261.

[33] Terri Moon Cronk, *China Poses Largest Long-Term Threat to U.S., DOD Policy Chief Says*, Dep't of Defense (Sept. 23, 2019), *available at* https://www.defense.gov/Explore/News/Article/Article/1968704/china-poses-largest-long-term-threat-to-us-dod-policy-chief-says/.

[34] Dep't of Defense, *DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021* (Oct. 5, 2022), *available at* https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.

[35] *Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment*, 85 Fed. Reg. 42,665 (Dep't Defense July 14, 2020).

[36] Section 4.2101(4) of *Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*, General Services Administration, *available at* https://www.acquisition.gov/far/subpart-4.21.

[37] Subpart 225.770 of *Defense Federal Acquisition Regulation Supplement*, Off. of the Sec'y of Defense (last revised Oct. 30, 2023), *available at* https://www.acq.osd.mil/dpap/dars/dfars/html/current/225_7.htm.

including the risk related to cyber-espionage or sabotage by entities identified by the U.S. Government "including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China."[38]

These regulations are seldom used to secure defense supply chains, let along commercial ones. At present are a number of Chinese military companies on the 1260H list, including Huawei, Inspur Group, and Semiconductor Manufacturing International Corporation ("SMIC") that enjoy significant commercial presence in the U.S. market. The exact extent to which their hardware remains in military systems remains is unknown given the purported inability of defense contractors, or "primes," to audit their full supply chains. The presence of Chinese hardware in military systems, including legacy military systems, is believed to be significant.

There are additional legal authorities that identify Chinese military companies under U.S. law, but they similarly fail to prohibit the use of these companies' hardware in U.S. systems. For instance, in 2021, President Biden issued E.O. 14032 entitled "Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China" which identified just over sixty "Chinese Military Industrial Complex" companies and Chinese companies involved with the development or use of surveillance technologies to facilitate repression or serious human rights abuses.[39] The E.O. prohibited certain U.S. public investments in the designated companies, but did not prohibit the use of hardware from these companies in U.S. commercial and defense systems.[40]

Additional legal authorities impose other types of prohibitions on activities with high-risk Chinese companies, including the Entity List (requiring U.S. Government licenses for exports of goods, software and technology), Section 889 of the 2019 National Defense Authorization Act (federal procurement prohibition), and Section 5949 of the 2023 National Defense Authorization Act (federal procurement prohibition).[41] Despite the fact that the hundreds of Chinese military and surveillance companies identified on these lists (although far from comprehensive) have each been deemed a U.S. national security risk, their presence and participation in the U.S. commercial and military sectors remains largely unregulated. For example, Chinese chip maker Hulan and its subsidiary Initio are on the U.S. Department of Commerce's Entity List, yet are still permitted to

---

[38] *Consolidated Appropriations Act, 2018*, Public Law 115-141, U.S. Congress (2018), *available at* https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

[39] White House, *Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China* (June 3, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.

[40] *Id.*

[41] Bureau of Industry and Security, U.S. Dep't of Commerce, *Entity List*, *available at* https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list; Off. of Foreign Assets Control, U.S. Dep't of the Treasury, *Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists*, *available at* https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists; Section 889 of the *National Defense Authorization Act for Fiscal Year 2019*, U.S. Congress (2019), *available at* https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf; Section 1260H of the *National Defense Authorization Act for Fiscal Year 2021*, U.S. Congress (2021), *available at* https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf; Section 5949 of the *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, U.S. Congress (2023), *available at* https://www.govinfo.gov/content/pkg/PLAW-117publ263/pdf/PLAW-117publ263.pdf.

supply encrypted hard drives to the U.S. Navy and numerous other North Atlantic Treaty Organization fighting forces. Hulan and Initio maintain concerning connections to the PLA, and their hard drives have multiple security vulnerabilities, potentially deliberately placed, identified by third party analysts.[42] For its part, semiconductors produced by SMIC, a Chinese company specifically designated under Section 5949 for federal government procurement bans, is likely prevalent in U.S. military systems but the U.S. Government is unable to identify where those chips are located. The lack of adequate domestic capacity to replace Chinese product is another factor frustrating the defense sector's ability to wean itself off Chinese chips.[43]

In addition to IT equipment, the DOD continues to use Chinese drones manufactured by DJI, a Chinese company designated to the Entity List, the 1260H list, and CMIC list.[44] The U.S. Government has long known that DJI's drones conduct surveillance activities in the United States and that the data obtained are shared with the Chinese government. In 2020, the U.S. Government also found that DJI was involved in forced labor in China.[45] Subsequently, the Uyghur Forced Labor Prevention Act ("UFLPA") became law in 2021 and banned the U.S. importation of products involved in forced labor. [46] Despite the UFLPA's import restrictions, imports of DJI drones continue to flow into the United States. And even though the UFLPA amended the Uyghur Human Rights Policy Act of 2020[47] to permit U.S. Government sanctions on companies involved in forced labor, the U.S. Government has declined to sanction DJI. Finally, despite the fact that certain U.S. investments in DJI are banned under the CMIC E.O., DJI's drones are permitted to roam freely and spy on communities across the United States.

Today, DJI accounts for well over 70% of the commercial drone use in the United States.[48] The remaining market share is held by another, lesser-known Chinese company named Autel Robotics, Inc., which similarly supplies both the commercial market as well as federal and state government bodies.[49] In an effort to address the pervasive presence of Chinese drones in the United States, the U.S. Government passed the American Security Drone Act ("ASDA") as part of the National

---

[42] Andy Greenberg, *How a Shady Chinese Firm's Encryption Chips Got Inside the US Navy, NATO, and NASA*, Wired (June 15, 2023), *available at* https://www.wired.com/story/hualan-encryption-chips-entity-list-china/.

[43] Alan Patterson, *Experts: U.S. Military Chip Supply Is Dangerously Low*, EE Times (Jan. 6, 2023), *available at* https://www.eetimes.com/experts-u-s-military-chip-supply-is-dangerously-low/.

[44] Chris Rodrigo and Maggie Miller, P*entagon report clears use of drones made by top Chinese manufacturer*, The Hill (June 1, 2021), *available at* https://thehill.com/policy/defense/556370-pentagon-report-clears-use-of-drones-made-by-top-chinese-manufacturer/.

[45] *Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List*, 85 Fed. Reg. 83,416 (Dep't Commerce Dec. 22, 2020)**Error! Hyperlink reference not valid.**.

[46] Uyghur Forced Labor Prevention Act in 2021, U.S. Congress (2021), *available at* https://www.govinfo.gov/content/pkg/PLAW-117publ78/pdf/PLAW-117publ78.pdf.

[47] Uyghur Human Rights Policy Act of 2020, U.S. Congress (2020), *available at* https://www.congress.gov/116/plaws/publ145/PLAW-116publ145.pdf.

[48] Nessa Anwar, *World largest done maker is unfazed – even if it's blacklisted by the U.S.*, CNBC (Feb. 7, 2023), *available at* https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html.

[49] Eric Sayers and Klon Kitchen, *DJI isn't the only Chinese drone threat to US security. Meet Autel.*, DefenseNews (Sept. 15, 2023), *available at* https://www.defensenews.com/opinion/2023/09/15/dji-isnt-the-only-chinese-drone-threat-to-us-security-meet-autel/.

Defense Authorization Act for Fiscal Year 2024.[50] Although the ASDA bans federal agencies from using federal funds to purchase or using drones made in or made with components from foreign countries of concern, including China, Iran, Russia, and North Korea,[51] the prohibitions on procurement and use do not kick in until December 2025 and last only through December 2028.[52] Further, many U.S. federal agencies have been exempt from complying with the ban and all agencies are able to apply for waivers in order to continue procuring and using covered drones. Finally, DJI and Autel have not been excluded from the U.S. commercial market through any legal measures, meaning that Chinese surveillance continues across the United States and the resulting threats to national security remain unaddressed.

Next, the DOD's modern vision for U.S. military doctrine, particularly its efforts to multiply U.S. airpower capabilities through increased used of unmanned autonomous aerial vehicle systems, similarly raises concern about America's reliance on Chinese hardware in these systems. DOD's recently announced Replicator Initiative, which is an initiative to field thousands of autonomous systems across a broad range of warfighting domains to counter China's rapid armed forces buildup, relies on the production and procurement of low-cost drones.[53] The DOD plans to have these drones online quickly within 18-24 months of the program's August 2023 announcement.[54] But, in light of China's existing dominance in aerial drone production and related hardware components, combined with the short timeline that the DOD has given for onboarding these aerial systems, there is reason for concern that many of the systems deployed in the Replicator Initiative will rely on Chinese hardware.[55]

The risks associated with relying on Chinese hardware and designs in U.S. military systems is self-evident and immense. Cyber-vulnerabilities enabled through Chinese hardware could render DOD platforms inoperable and unavailable to respond to potentially hostile Chinese action.[56] In a sophisticated operation, outside actors may even be capable of gaining access to U.S. systems and directing them to harm military and civilian targets.[57]

---

[50] National Defense Authorization Act for Fiscal Year 2024, U.S. Congress (2024), *available at* https://www.govinfo.gov/content/pkg/BILLS-118hr2670rh/pdf/BILLS-118hr2670rh.pdf.

[51] Zacc Dukowitz, *A Federal DJI Ban Is Coming–Here's Why It Matters*, UAV Coach (Dec. 20, 2023), *available at* https://uavcoach.com/asda-law/.

[52] Eric Holdeman, *Federal Government Will Require Purchase of 'Made in America' Drones*, Government Technology (Jan. 8, 2024), *available at* https://www.govtech.com/em/emergency-blogs/disaster-zone/federal-government-will-require-purchase-of-made-in-america-drones.

[53] Chris Gordon and John Tirpak, *Pentagon Wants to Buy 1,000s of Small, Cheap, Autonomous Drones in Next Two Years*, Air & Space Forces Magazine (Aug. 28, 2023), *available at* https://www.airandspaceforces.com/pentagon-replicator-small-cheap-autonomous-drones/.

[54] *Id.*

[55] Eva Dou and Gerrit De Vynck, *Pentagon plans a drone army to counter China's market dominance*, The Washington Post (Dec. 1, 2023), *available at* https://www.washingtonpost.com/technology/2023/12/01/pentagon-drones-replicator-ukraine/.

[56] Lukas Olejnik, *The Dire Possibility of Cyberattacks on Weapons Systems*, Wired (Mar. 10, 2021), *available at* https://www.wired.com/story/dire-possibility-cyberattacks-weapons-systems/.

[57] *Id.*

As already noted, at the heart of the DOD's struggle with Chinese hardware is its continued failure to develop a robust and economically secure domestic manufacturing base. The DOD continues to prioritize low-costs items, and the Pentagon as an institution incentivizes a military-industrial base that cannot respond to potential needs for mass production. A select few large companies fulfill procurement for low-volume and highly-tailored equipment, and the remaining items are generally outsourced.[58] Even when larger DOD suppliers are involved, they rely on secondary and tertiary suppliers for hardware components, which are increasingly difficult to find in the United States as orders and margins are too small and too inconsistent to sustain domestic production capacities.[59] With the concentration of hardware supply chains in China, DOD suppliers often have no choice but to resort to Chinese hardware for their systems. This, of course, renders defense systems vulnerable to potential cyberattacks and system failures.[60]

C. Water Facilities and Energy Utilities

Utilities are increasingly relying on outsourced computing and automation hardware, and consequently becoming susceptible to foreign exploitation of their internal systems.

a. Water Treatment Facilities

Water treatment plants increasingly utilize automated systems to perform treatment processes that deliver safe and potable water.[61] If commandeered by hostile actors, automated systems can cause significant disruption to municipal water supplies including limiting access to water or producing toxic, contaminated water.[62] In February 2021, an employee at the Bruce T. Haddock Water Treatment Plant in Oldsmar, Florida reported unauthorized access to the plant's control and an attempt to raise the amount of lye in the plant's treated water to toxic levels.[63] Although an investigation never publicly identified a culprit for the alleged incident, experts on critical infrastructure systems concede that cyberattacks are a threat.[64] The degree to which American water treatment facilities utilize Chinese hardware and related software is difficult to determine, but trends in the water treatment industry point to an increased reliance on Chinese components for plant operations.

---

58 Govini Report.

59 *Id.*

60 *Id.*

61 Idrica, *Water Trends in automation for 2023: Improving operability and management* (Mar. 7, 2023), *available at* https://www.idrica.com/blog/water-trends-in-automation-for-2023-improving-operability-and-management/#:~:text=In%202023%2C%20and%20in%20the,different%20DWTP%20processes%20in%20isolation.

62 Cybersecurity & Infrastructure Security Agency, *Water and Wastewater Systems*, *available at* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector.

63 Cybersecurity & Infrastructure Security Agency, *Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility* (Feb. 12, 2021), *available at* https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a.

64 Christian Vasquez, *Did someone really hack into the Oldsmar, Florida, water treatment plant? New details suggest maybe not*, CyberScoop (Apr. 10, 2023), *available at* https://cyberscoop.com/water-oldsmar-incident-cyberattack/.

Water treatment facilities across the United States are increasingly adopting autonomous and networked systems, such as supervisory control and data systems ("SCADA") and IoT devices, such as smart readers, to operate water treatment systems independent of human input.[65] The CCP, for its part, has prioritized industrial automation as an essential sector and, so, has dedicated significant funding to advancing its domestic SCADA manufacturing capabilities. In fact, the CCP highlighted industrial automation in its last two Five-year Plans and identified automation as one of the ten key industries in its Made in China 2025 ("MIC 2025") initiative.[66] CCP-funded government guidance funds tied to the MIC 2025 have registered a capital target of $1.5 trillion and had raised $627 billion of that target as of 2020.[67] Beyond direct funding, the CCP assists MIC 2025 entities through tax, trade, and investment measures, forced joint ventures and partnerships, technology licensing and equipment, and talent recruitment and training assistance. [68] These programs are organized to mature Chinese industries more quickly than competitors. [69] They are also designed to provide low-cost alternatives to markets globally, including SCADA. Beyond economic gains, the CCP's motivation is to export systems that enable backdoor access to other countries' critical infrastructure, which could then be leveraged at any time to gain an upper hand in a conflict. Chinese hardware in automated systems is a significant concern for the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), among other cybersecurity organizations, which identifies SCADA and other industrial control systems in critical infrastructure as particularly vulnerable to cybersecurity risks.[70]

It is likely that American water treatment facilities, where cybersecurity oversight at the state and federal level is limited, are already using Chinese SCADA systems and components in their automated facilities, rendering the systems vulnerable to dangerous cybersecurity attacks.[71] Water treatment facilities that serve smaller and more rural communities are even more likely to utilize

---

[65] Inductive Automation, *SCADA: Supervisory Control and Data Acquisition: What is SCADA, Who Uses it and How SCADA Has Evolved* (Sept. 12, 2018), *available at* https://inductiveautomation.com/resources/article/what-is-scada.

[66] *See* Stanford University, *Translation: 14th Five-Year Plan for National Informatization – Dec. 2021*, *available at* https://digichina.stanford.edu/wp-content/uploads/2022/01/DigiChina-14th-Five-Year-Plan-for-National-Informatization.pdf; Nat'l Dev. and Reform Comm'n., *The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China*, *available at* https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf; Center for Security and Emerging Technology, Georgetown University, *Translated: Made in China 2025*, *available at* https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf; *see also* Outlier Automation, *How China Became an Industrial Automation Powerhouse* (Feb. 1, 2022), *available at* https://www.outlierautomation.com/blog/how-china-became-an-industrial-automation-powerhouse.

[67] Congressional Research Service, *"Made in China 2025" Industrial Policies: Issues for Congress* (last updated Mar. 10, 2023) at 2, *available at* https://sgp.fas.org/crs/row/IF10964.pdf.

[68] *Id.*

[69] Shaoshan Liu, *China's Pursuit of Autonomous Machine Computing Self-Sufficiency*, The Diplomat (Nov. 17, 2023), *available at* https://thediplomat.com/2023/11/chinas-pursuit-of-autonomous-machine-computing-self-sufficiency/.

[70] Cyber Security & Infrastructure Security Agency, Industrial Control Systems, *available at* https://www.cisa.gov/topics/industrial-control-systems.

[71] Robert F. Powelson, *Without federal action, hackers will continue to endanger US water systems*, The Hill (Dec. 24, 2023), *available at* https://thehill.com/opinion/cybersecurity/4373600-without-federal-action-hackers-will-continue-to-endanger-us-water-systems/.

Chinese hardware given their lower costs and weaker cybersecurity software controls.[72] The foregoing risks to the water infrastructure have not been adequately addressed by federal and state governments. Cybersecurity requirements are at best extremely lax or, in large part, nonexistent.

b. U.S. Energy Providers and the Electricity Grid

For several years, Members of Congress, executive agencies, and third-party organizations have been sounding the alarm on the potential risks caused by Chinese components and hardware embedded into U.S. energy grid. In testimony before the Senate Energy and Natural Resources Committee, Director of CESAR (the Department of Energy's ("DOE") Office of Cybersecurity, Energy Security, and Emergency Response) Puesh Kumar, pointed to reports from the Director of National Intelligence ("DNI") and emphasized that cyber actors are targeting U.S. energy infrastructure, and they are posing serious threats to national security.[73] Further, the 2023 Annual Threat assessment from DNI identified China as representing "the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks [and that] China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland."[74]

Today, outsider actors are capable of exploiting hardware vulnerabilities in U.S. systems to destroy physical components of the U.S. electric grid.[75] The attacks could originate from hardware within the grid itself, or the transmission of malicious code to the grid from external hardware devices, such as electric vehicles ("EV") charging stations, large data and power storage devices, or telecommunication equipment scattered nationwide. Large attacks on the U.S. electric grid, should they occur, will have devastating impact on the United States population – leaving masses without access to electricity and heat and will cause critical service systems such as hospitals, emergency services, utility providers (water/sewer, gas), and military installations incapable of performing essential tasks.[76] Attacks on military utility installations have been a particular area of concern as hostile nations could utilize preemptive blackouts to limit U.S. defensive and responsive capabilities.

---

[72] *See* Robert F. Powelson, *Without federal action, hackers will continue to endanger US water systems*, The Hill (Dec. 24, 2023), *available at* https://thehill.com/opinion/cybersecurity/4373600-without-federal-action-hackers-will-continue-to-endanger-us-water-systems/; Connor Griffin, *Billions for Water Infrastructure, but Small Communities Risk Being Left Out to Dry*, Governing (June 23, 2023), *available at* https://www.governing.com/infrastructure/billions-for-water-infrastructure-but-small-communities-risk-being-left-out-to-dry.

[73] *Cybersecurity Vulnerabilities to the United States' Energy Infrastructure*, Hearing Before the Senate Energy and Natural Resources Committee, 118th Cong. (Mar. 23, 2023) (testimony of Puesh Kumar, Director, Off. of Cybersecurity, Energy Security, and Emergency Response, Dep't of Energy), *available at* https://www.energy.senate.gov/services/files/7C2EC274-467C-4444-BD14-D4F11E474492.

[74] Off. of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[75] Andy Greenberg, *How 30 Lines of Code Blew Up a 27-Ton Generator*, Wired (Oct. 23, 2020), *available at* https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/.

[76] Senate Republican Policy Committee, *Infrastructure Cybersecurity: The U.S. Electric Grid* (July 16, 2021), *available at* https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-the-us-electric-grid.

Moreover, power plants and petrochemical refineries and facilities may similarly be rendered inoperable due to cyber intrusions.[77] And nuclear generation facilities, in particular, pose a risk for catastrophic destruction should outside interference induce a radiological release.[78] These are merely a few examples of the range of risks that exist today. These risks become all the more dangerous when coordinated cyberattacks simultaneously cripple multiple power sources across broad geographic regions.

In the DOE's 2021 Prohibition Order Securing Critical Defense Facilities, the DOE correctly observed that attacks may be leveraged preemptively to handicap the U.S. defense posture: *"Such attacks are most likely during crises abroad where Chinese military planning envisions early cyberattacks against the electric power grids around CDFs in the U.S. to prevent the deployment of military forces and to incur domestic turmoil.*" [79] Consequently, the DOE is attempting to identify vulnerabilities in energy systems at the subcomponent level, by identifying which components are manufactured in China by testing equipment "down to the chips level" with the support of DOE-partnered laboratories.[80]

It is likely that the DOE will find a large number of Chinese hardware in its systems, but then what will it propose to do? To date, the DOE has not made any concerted effort to remove Chinese components from the domestic energy infrastructure. Previously in 2020, President Trump issued an E.O. prohibiting the acquisition, importation, transfer, or installation of specified bulk-power system electric equipment from China (and other adversaries) that directly serve Critical Defense Facilities ("CDF"s).[81] The Biden Administration subsequently revoked the E.O. and has not yet addressed the threat to CDFs.[82] The power supply for military installations will continue to be vulnerable as long as Chinese hardware remains in use, so inaction is not an option.

It has been reported that some non-defense utility companies in the United States have already, to varying degrees, recognized the threats posed by the use of Chinese hardware and have begun to look for alternatives.[83] To the extent this is true, and even if Chinese hardware is fully removed

---

77 Katie Benner and Kate Conger, *U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant*, New York Times (Mar. 24, 2022), *available at* https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html#:~:text=WASHINGTON%20%E2%80%94%20The%20Justice%20Department%20unsealed,petrochemical%20facility%20in%20Saudi%20Arabia.

78 Susan Pickering and Peter Davies, *Cyber Security of Nuclear Power Plants: US and Global Perspectives*, Georgetown Journal of International Affairs (Jan. 22, 2021), *available at* https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/.

79 *Prohibition Order Securing Critical Defense Facilities*, 86 Fed. Reg. 533 (Dep't Energy Jan. 6, 2021).

80 Robert Walton, *DOE cyber chief gets bipartisan grilling as senators question US reliance on China for grid equipment*, Utility Dive (Mar. 24, 2023), *available at* https://www.utilitydive.com/news/doe-cyber-chief-bipartisan-grilling-senators-china-power-grid-transformers/645914/.

81 *Exec. Order 13920*, 85 Fed. Reg. 26,595 (Exec. Off. May 1, 2020); *Prohibition Order Securing Critical Defense Facilities*, 86 Fed. Reg. 533 (Dep't Energy Jan. 6, 2021).

82 *Revocation of Prohibition Order Securing Critical Defense Facilities*, 86 Fed. Reg. 21,308 (Dep't Energy Apr. 22, 2021).

83 Michael Novinson, *US Officials Urged to Examine Chinese Risk to Electric Grid*, Bank Info Security (Mar. 23, 2023), *available at* https://www.bankinfosecurity.com/us-officials-urged-to-examine-chinese-risk-to-electric-grid-a-21508.

from the energy grid, the fact remains that external devices containing Chinese hardware (e.g., EV charging station) can connect to the grid and transfer malicious software to the grid. This remote-access issue is another dimension of the problem that remains to be addressed.

It should also be noted that renewable energy is also an area where Chinese hardware can pose a potential vulnerability. As solar energy's role in domestic energy production continues to grow to meet America's climate goals, so does the share of the U.S. solar market controlled by Chinese panel makers.[84] Inverters required for solar energy production are particularly vulnerable to cyber exploitation.[85] China is the top producer of inverters in the U.S. market, and Huawei, already known for its cooperation with the CCP, is the world's largest producer of inverters.[86] In Australia, where the domestic solar market is even more dependent on Chinese solar companies than the United States,[87] the national government has received increasing calls to assess the cybersecurity vulnerabilities of relying on Chinese hardware for solar production.[88] China's domination of the global wind tower market poses similar threats.

Finally, large energy material producers, including petrochemical facilities, face similar vulnerabilities to water treatment facilities due to their increasing reliance on industrial automation including SCADA technologies.[89] As China continues to expand its role as a supplier of industrial automation systems, production facilities will increasingly adopt Chinese hardware in their internal systems, raising the risk that cyberattacks will render these systems inoperable.

D. Public Transportation

In 2020, Congress passed the Transit Infrastructure Vehicle Security Act into law, which barred transit agencies from using federal funds to purchase Chinese rolling stock or buses manufactured

---

84 Phred Dvorak, *China's Dominance Over U.S. Solar Market Grows Despite Efforts to Stem It*, Wall Street Journal (Apr. 26, 2023), *available at* https://www.wsj.com/articles/china-dominates-u-s-solar-market-as-lawmakers-tussle-over-tariffs-7c2d749d.

85 Raymond Watts and Brian Kline, *Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors*, Ridge Global (Oct. 29, 2018), *available at* https://protectourpower.org/resources/ridge-global-report-2018.pdf; *see also* Andrew Smith, *Former US Homeland chief warns Chinese solar inverters pose cyber threat*, S&P Global (Nov. 6, 2018), *available at* https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/former-us-homeland-chief-warns-chinese-solar-inverters-pose-cyber-threat-47589890 ("S&P Report").

86 S&P Report.

87 Jayant Chakravarti, *Australia Focuses on Threat of Chinese Attack on Solar Power*, Bank Info Security (Oct. 25, 2023), *available at* https://www.bankinfosecurity.com/australia-focuses-on-threat-chinese-attack-on-solar-power-a-23395#:~:text=China%20dominates%20the%20Australian%20solar,to%20renewable%20sources%20by%202028.

88 Cindy Li, *Australian Government Urged to Assess Chinese Solar Panels Over Cybersecurity Concerns*, The Epoch Times (Aug. 10, 2023), *available at* https://www.theepochtimes.com/world/australian-government-urged-to-assess-chinese-solar-panels-over-cybersecurity-concerns-5456025.

89 *See* Gregory Miller, *Automation: a positive force in the power sector*, Power Electronic News (July 26, 2019), *available at* https://www.powerelectronicsnews.com/automation-a-positive-force-in-the-power-sector/; *see also* INDUSTLABS, *The Importance of Automation in the Oil & Gas Industry* (Jan. 12, 2023), *available at* https://industlabs.com/news/oil-and-gas-automation#:~:text=SCADA%20Systems,make%20trips%20to%20the%20sites.

by state-owned, controlled, or subsidized companies.[90] However, several of America's largest transit systems use Chinese rolling stock or will be supplied with Chinese rolling stock as part of contracts signed before the 2020 ban.[91] Four of America's largest cities, Boston, Chicago, Philadelphia, and Los Angeles, utilize rolling stock produced by the China Railway Rolling Stock Corp., China's largest producer.[92] Beyond rolling stock, a 2022 Center for Security and Emerging Technology report also flagged that a number of U.S. transit agencies have procured information and communications technology and services hardware from covered entities such as Huawei and ZTE.[93]

U.S. transit systems' utilization of Chinese hardware presents yet another major cyber vulnerability. Transit rail is highly networked and often coordinated at a system-wide level.[94] A hostile actor with access to a specific network vulnerability could exploit it to disrupt or damage major U.S. transit systems or cause rolling stock to deliberately derail or collide.[95] In addition, transit agencies maintain a sizable amount of riders' personal information, including their names, addresses, emails, and payment information. Chinese actors certainly have the ability and motivation to exploit network vulnerabilities to access such user information for surveillance purposes, financial gains, or other reasons. U.S. laws are ultimately inadequate to protect America from these risks as well.[96]

---

[90] *Transit Infrastructure Vehicle Security Act*, U.S. Congress, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/846?q=%7B%22search%22%3A%22H.R.+3%22%7D&s=1&r=76; *see also* Off. of Congressman Eric Swalwell, Swalwell, Garamendi Introduce Legislation to Secure FAA Transit Vehicles from Chinese Ownership (Apr. 26, 2023), *available at* https://swalwell.house.gov/media-center/press-releases/swalwell-garamendi-introduce-legislation-secure-faa-transit-vehicles#:~:text=The%20Transit%20Infrastructure%20Vehicle%20Security,%2C%20controlled%2C%20or%20subsidized%20companies.

[91] Zhong Nan, *Chinese maker delivers 1st of 400 subway cars for Chicago*, China Daily (last updated July 9, 2022), *available at* https://www.chinadaily.com.cn/a/202206/09/WS62a12d1ba310fd2b29e61855.html#:~:text=CRRC%2C%20China's%20largest%20rolling%20stock,Chicago%2C%20Philadelphia%20and%20Los%20Angeles.

[92] *Id.*

[93] Jack Corrigan, Sergio Fontanez, and Michael Kratsios, *Banned in D.C.: Examining Government Approaches to Foreign Technology Threats*, Center for Security and Emerging Technology (Oct. 2022), *available at* https://cset.georgetown.edu/wp-content/uploads/CSET-Banned-in-D.C.-1.pdf.

[94] *See* Washington Professional Systems, *Washington Metro Area Transit Authority – Rail Operations Control Center (ROCC)*, *available at* https://wpsproav.com/integration-case-studies/washington-metro-area-transit-authority/.

[95] Paulina Okunyte, *Infrastructure at risk: can trains be hacked*, Cybernews (Nov. 15, 2023), *available at* https://cybernews.com/editorial/train-hacking-explained/.

[96] Nassim Benchaabane, *Hackers steal data and demand ransom from Metro Transit in St. Louis*, St. Louis Post-Dispatch (Oct. 12, 2023), *available at* https://www.stltoday.com/news/local/crime-courts/hackers-steal-data-and-demand-ransom-from-metro-transit-in-st-louis/article_97f4ed36-67bb-11ee-9e48-4fcfe5eaa7ac.html.

E. Passenger Vehicles

Over the past two decades, automotive manufacturers have installed an ever-larger number of computer hardware components in the U.S. passenger vehicle fleet.[97] While the additional hardware has allowed the addition of numerous quality-of-life and safety improvements, the connection of many modern vehicles to the Internet enables outside actors to exploit their internal processes.[98] These hostile actors are able to exploit passenger vehicle vulnerabilities to leave vehicles inoperable,[99] cause vehicles to crash,[100] or cause EV batteries explode.[101] As vehicles become more interconnected, moreover, vulnerabilities can be exploited in order to launch a coordinated attack that renders fleets of vehicles simultaneously inoperable crippling U.S. defense capabilities and leaving populations hostage in the event of a kinetic attack.[102]

Moreover, as original equipment manufacturers ("OEM") include additional microelectronic features to augment their vehicles' electronic capabilities, users become more vulnerable to unknown entities accessing their personal information stored on vehicle computer systems without their authorization.[103] Even when OEMs claim to have full access to the vehicle's data, the foreign-origin components in automotive parts are likely to have embedded backdoors that allow infiltration by malign actors.

The degree to which U.S. automakers utilize Chinese hardware in the U.S. passenger vehicles is difficult to determine and may be part of the Commerce Department's recently announced semiconductor industrial base assessment.[104] Whatever the outcome of the agency's assessment, it is abundantly clear at the moment that China's semiconductor industry is well-positioned to dominate the auto chip sector. As the majority of semiconductors used in passenger vehicles are

---

97 *See* Wired, *Cars Are Just Software Now* (Oct. 20, 2022), *available at* https://www.wired.com/story/gadget-lab-podcast-571/#:~:text=This%20week%2C%20we%20discuss%20how,drive%2C%20and%20maintain%20our%20vehicles.&text=Modern%20cars%20are%20giant%20computers,%2C%20safer%2C%20and%20more%20comfortable.

98 U.S. Dep't of Transportation, *Connected Vehicles and Cybersecurity*, *available at* https://www.its.dot.gov/factsheets/pdf/cv_%20cybersecurity.pdf.

99 Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, Wired (Mar. 17, 2018), *available at* https://www.wired.com/2010/03/hacker-bricks-cars/.

100 Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (July 21, 2015), *available at* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

101 Bart Ziegler, *Could Electric Vehicles Be Hacked?*, The Wall Street Journal (Feb. 14, 2023), *available at* https://www.wsj.com/articles/could-electric-vehicles-be-hacked-71a543e3.

102 Georgia Institute of Technology, News Release, *Hackers could use connected cars to gridlock whole cities* (July 28, 2019), *available at* https://www.eurekalert.org/news-releases/697837.

103 Patrick George, *Car Hackers Are Out for Blood,* The Atlantic (Sept. 11, 2023), *available at* https://www.theatlantic.com/technology/archive/2023/09/electric-car-hacking-digital-features-cyberattacks/675284/.

104 Press Release, U.S. Dep't of Commerce, Office of Public Affairs, Commerce Department Announces Industrial Base Survey of American Semiconductor Supply Chain (Dec. 21, 2023), *available at* https://www.commerce.gov/news/press-releases/2023/12/commerce-department-announces-industrial-base-survey-american.

legacy chips,[105]China has been rapidly expanding its production of these chips so that by 2027, it is estimated to control at least 33% of all legacy chip production worldwide.[106] China's focus on automotive semiconductor production stems, in part, from its need to support its growing OEM sector.[107] China's 2027 plans to engage in overcapacity, however, are nefarious and intended to distort global markets. To be clear, China has been a significant producer of legacy semiconductors and other electronic auto components for many years, and its products have been prevalent in most American and European vehicles since at least 2012-2015.[108] But, to date, very little has been done to mitigate the associated risks.

F. Election Infrastructure

Hardware and software vulnerabilities in the American voting system are likewise a very serious threat that should be addressed before the elections this year.[109] Voting systems are concentrated targets for attack,[110] and there are numerous hardware and software points of access to voting systems, including the individual voting machines, election-management systems (which are small networks of computers operated by state or county governments or outside vendors), and memory cards or USB sticks for the voting machines.[111] More than 30 states allow voters to cast electronic ballots, but many do not have basic security measures like encryption.[112] There are many additional gaps in election security, particularly in polling place equipment, that render large parts of the U.S. voting apparatus vulnerable to foreign interference.[113] More needs to be done to protect the integrity of Americans' ballots.

Congress and industry experts have already found that voting machines typically contain foreign-made chips and are particularly vulnerable to interference. The Senate Intelligence Committee

---

[105] Sujai Shivakuma, Charles Wessner, and Thomas Howell, *The Strategic Importance of Legacy Chips*, Center for Strategic and International Studies (Mar. 3, 2023), *available at* https://www.csis.org/analysis/strategic-importance-legacy-chips.

[106] *Id.*; Joanne Chiao and Eden Chung, *China's Share in Mature Process Capacity Predicted to Hit 29% in 2023, Climbing to 33% by 2027*, TrendForce (Oct. 18, 2023), *available at* https://www.trendforce.com/presscenter/news/20231018-11889.html.

[107] Jeff Pao, *Will US target China's auto chip supply next?,* Asia Times (Oct. 29, 2022), *available at* https://asiatimes.com/2022/10/will-us-target-chinas-auto-chip-supply-next/; Sarah Wu, Jane Lee, and Kevin Krolicki, *Insight: How China became ground zero for the auto chip shortage*, Reuters (July 19, 2022), *available at* https://www.reuters.com/business/autos-transportation/how-china-became-ground-zero-auto-chip-shortage-2022-07-18/#:~:text=The%20scramble%20for%20workarounds%20has,maker%20and%20an%20auto%20supplier.

[108] CBS News, *Ford Motor loses $3.1 billion due to chip shortage and Rivian* (Apr. 27, 2022), *available at* https://www.cbsnews.com/news/ford-motor-losses-chip-shortage-rivian/.

[109] *See* Christina Cassidy, *Voting experts warn of 'serious threats' for 2024 from election equipment software breaches*, Associated Press (Dec. 5, 2023), *available at* https://www.pbs.org/newshour/politics/voting-experts-warn-of-serious-threats-for-2024-from-election-equipment-software-breaches.

[110] *Id.*

[111] *See id.*

[112] Jerod Macdonald-Evoy, *In the absence of national regulations, how vulnerable is our voting infrastructure?*, Arizona Mirror (Sept. 24, 2020), *available at* https://www.azmirror.com/2020/09/24/in-the-absence-of-national-regulations-how-vulnerable-is-our-voting-infrastructure/.

[113] *See, e.g.*, Jen Schwartz, *The Vulnerabilities of our Voting Machines*, Scientific American (Nov. 1, 2018), *available at* https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/

found significant supply chain vulnerabilities in voting machines in 2018.[114] A separate study found that some had security features turned off when they were shipped and used unencrypted hard drives.[115] A another study by a supply chain monitoring company found that a voting machine widely used in the United States from an unnamed vendor contained parts made by companies with ties to Russia and China. Despite pushback from the prominent American voting-machine suppliers, including Election Systems & Software, Dominion Voting Systems, and Hart InterCivic,[116] the report drew attention from the Hill and news outlets.

In January 2020, the CEOs of all three top voting-machine vendors testified before the Committee on House Administration of the U.S. House of Representatives.[117] Tom Burt, the CEO of Election Systems & Software, acknowledged that programmable logic devices for DS200 polling place ballot scanner are produced at a factory in China.[118] Additionally, John Poulos, CEO of Dominion Voting Systems, testified that his company sources "chip component level" inputs from China. He further indicated that there is currently no option for manufacturing some of these components in the United States. Julie Mathis, CEO of Hart InterCivic, concurred with Poulos on the supply chain issues and necessity of sourcing chips and other hardware components from China. All three CEOs conceded during the hearing that they would welcome guidance, comprehensive regulations, and reporting requirements from the federal government to protect the integrity of the U.S. voting system. There are currently no national guidelines for the procurement of voting machine components, for enhanced cybersecurity measures, or for local election officials to conduct audits or tests on electronic voting devices.[119]

The stream of coverage of these vulnerabilities since the 2016 election also has the effect of decreasing voter confidence in our election process.[120] The UCISA found that voting machines from Dominion Voting Systems used in at least 16 states had cybersecurity vulnerabilities that left them susceptible to hacking.[121] Particularly in the cybersecurity space, there is a low bar for supply

---

114 Alexa Corse, *Voting – Machine Parts Made by Foreign Suppliers Stir Security Concerns*, Wall Street Journal (Dec. 17, 2019), *available at* https://www.wsj.com/articles/voting-machine-parts-made-by-foreign-suppliers-stir-security-concerns-11576494003.

115 *See* Arizona Mirror, *supra* note 110.

116 Michaela Ross, *Chinese Technology in Voting Machines Seen as Emerging Threat*, Bloomberg Law (Jan. 9, 2020), *available at* https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/XADVSQES000000?bna_news_filter=privacy-and-data-security#jcite.

117 *See 2020 Election Security – Perspectives from Voting System Vendors and Experts*, 116th Cong. (Jan. 9, 2020), *available at* https://www.govinfo.gov/content/pkg/CHRG-116hhrg41318/html/CHRG-116hhrg41318.htm.

118 *See id.*; *see* Ben Popken, Cynthia McFadden, and Kevin Monahan, *Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines*, NBC News (Dec. 19, 2019), *available at* https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516.

119 *See* Arizona Mirror, *supra* note 110.

120 *See* Scientific American, *supra* note 111.

121 Kate Brumback, *Voting software in some states is vulnerable to hacking, U.S. cyber agency says*, Fortune (May 31, 2022), *available at* https://fortune.com/2022/05/31/voting-software-vulnerable-hacking/.

chain attacks.[122] The advent of AI creates an additional need to address threats and implement best practices for hardware and software. With vulnerabilities rampant and foreign meddlers already exaggerating the effects of attacks to spread misinformation, immediate action is necessary.[123]

In the 2020 hearing before the House, the CEO of Hart InterCivic asserted that a "sea change" would be necessary in global technology supply chains for the U.S. to produce the parts needed for voting machines. The time for that "sea change" has come.

G. Emergency Services and Medical Equipment

In addition to the long list of risks that result from significant U.S. dependence on Chinese hardware, the American Hospital Association's Center for Health Innovation recently pointed out that cyber threats to hospitals are grave and are directly influenced by the geopolitical climate.[124] Existing vulnerabilities from Chinese hardware in computer systems and medical equipment may be readily exploited to cripple healthcare systems. Ransomware attacks, which have affected hospitals and healthcare companies, provide an example of the potential impact of such vulnerabilities.[125] Experts predict that medical equipment and devices will increasingly become targets for malicious attacks, as health record management systems improve their ability to resist efforts to steal patient records.[126] For instance, malign actors can attack pacemakers to deliver lethal electric shocks to patients, and they can manipulate drug infusion and insulin pumps to deliver lethal doses.[127]

The House of Representatives China Select committee has already noted that China has the ability to access and remotely control U.S. medical equipment if the equipment contains Chinese-made cellular modules.[128] In recognition of such risks, the U.S. Food and Drug Administration ("FDA") is now requiring manufacturers to submit plans to address cybersecurity vulnerabilities for any

---

[122] Ashlee Benge, *Software Supply Chain Risks Loom Over Elections Systems*, SpiceWorks (Nov. 14, 2023), *available at* https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/software-supply-chain-risks-loom-over-elections-systems/.

[123] Frank Bajak, *EXPLAINER: Threats to US election security grow more complex*, Associated Press (Nov. 2, 2022), *available at* https://apnews.com/article/2022-midterm-elections-technology-d6bf92f594343d7a489d40394e56e2a1.

[124] John Riggi, *Ransomware Attacks on Hospitals Have Changed*, AHA Center for Health Innovation (June 12, 2020), *available at* https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.

[125] *See* Ryan Levi, *Ransomware attacks against hospitals put patients' lives at risk, researchers say*, NPR (Oct. 20, 2023), *available at* https://www.npr.org/2023/10/20/1207367397/ransomware-attacks-against-hospitals-put-patients-lives-at-risk-researchers-say.

[126] Tina Reed, *"A real Achilles' heel": Medical devices could be hacked next, officials fear*, Axios (Jan. 4, 2024), *available at* https://www.axios.com/2024/01/04/hackers-health-care-cybersecurity-medical-devices.

[127] Peter Jaret, *Exposing vulnerabilities: How hackers could target your medical devices*, AAMC News (Nov. 12, 2018), *available at* https://www.aamc.org/news/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices.

[128] David Shepardson, *Two US lawmakers raise security concerns about Chinese cellular modules*, Reuters (Aug. 8, 2023), *available at* https://www.reuters.com/world/us/lawmakers-want-us-address-security-concerns-about-chinese-cellular-modules-2023-08-08/.

new medical devices.[129] The security requirements, passed as part of the December 2022 omnibus spending bill, require that all new medical device applicants to report how they intend to "monitor, identify, and address" cybersecurity issues and to provide the FDA with a "software bill of materials."[130] However, these FDA requirements do not apply to devices already on the market, nor do they adequately address the supply chain for hardware components.[131] There are also requirements to strengthen cybersecurity measures to prevent attacks. The American medical equipment system has substantial vulnerabilities that to date remain ignored and significantly unaddressed.

IV. POLICY RECOMMENDATIONS

What the forgoing discussion demonstrates is that the current capabilities of the United States' adversaries in the hardware-enabled cybersecurity domain is far greater than the United States'. China in particular is far better positioned to infiltrate our systems than we are to infiltrate theirs. Indeed, China controls the global supply chains for critical hardware components, and Chinese companies have their government's support to continue dominating the global markets in critical high-tech sectors. And whereas the CCP gives its national champions significant competitive advantages through heavy industrial subsidies and protections through aggressive market access barriers for foreign competitors, the United States welcomes cheap Chinese imports into its borders and does little to protect American industries that are injured by China's predatory economic practices.

As a result, America has ceded too much manufacturing capacity and technology to China over the past 20 years, and it needs to reverse this trend before it is too late. The U.S. Government needs a new policy mindset to strengthen its industrial base, and contrary to widespread belief, the solution is neither difficult nor impossible.

There exist today a broad range of effective legal authorities that can be – and ought to be – leveraged to restrict the U.S. importation and use of components sourced from China and other foreign adversaries. In particular, the E.O. entitled "Securing the Information and Communications Technology and Services Supply Chain"[132] is structured to prevent the use of high-risk Chinese hardware in U.S. telecommunications systems. The E.O. was issued in 2019 pursuant to the International Emergency Economic Powers Act ("IEEPA"), a federal law authorizing the president to regulate international commerce during peacetime after declaring a national emergency in response to any unusual and extraordinary threat to the United States. The E.O. was groundbreaking in that it represented the first time IEEPA was used to prohibit transactions involving information and communications technology or services ("ICTS") provided by foreign adversaries. More specifically, the E.O. authorizes the Commerce Department to prohibit transactions that involve ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary whenever the

---

129 *Id.*

130 Jennifer Korn, *FDA requires medical devices be secured against cyberattacks*, CNN (Mar. 29, 2023), *available at* https://www.cnn.com/2023/03/29/tech/fda-medical-devices-secured-cyberattacks/index.html.

131 *See id.*

132 White House, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019), *available at* https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Government determines that such a transaction, or a class of transactions poses a serious risk to U.S. national security. At this time, the E.O. has been in existence for nearly four years. Although the threats posed by ICTS transactions with Chinese entities increase exponentially day by day, the E.O. has not yet been leveraged to prohibit *any* high-risk transactions.

Apart from forming the legal basis of the ICTS E.O., IEEPA is, by itself, a powerful and flexible legal authority. IEEPA grants to the President broad authority to regulate commerce for national security reasons. With respect to risks to critical domestic capabilities, including commercial items as well as infrastructure and defense systems, IEEPA can be used to prevent transactions with Chinese and other foreign malign entities. Even though IEEPA is valid law today, it has not yet been used to protect critical national security systems from Chinese infiltration.

To the extent the U.S. Government is reluctant to use these legal authorities to prohibit transactions with Chinese entities due to concerns about the absence of domestic production to meet supply chain needs, several points are in order. First, whenever national security risks are at issue, inaction is not an option; solutions must be found and implemented before catastrophic events take place. Second, the United States enjoyed strong and resilient supply chains merely 20 years ago before manufacturing capacity gradually offshored to China. In fact, 20 years is not too far off in history, which means that America has the ability replicate resilient supply chains onshore once again. Through incentive programs like the CHIPS Act, the Inflation Reduction Act, the Bipartisan Infrastructure and Jobs Act, and other federal award programs, the U.S. Government should focus on the manufacturing capabilities necessary to strengthen and sustain the *defense* industrial base. From the national security standpoint, priority sectors should include hardware necessary to support defense systems (e.g., integrated circuits for weapons systems) as well as leap ahead technologies that enable the United States to gain technological leadership over global competitors (e.g., leading edge chips).

Furthermore, given that Government resources are limited, federal awards may not be available to support manufacturing capacity for purely *commercial* hardware. Nevertheless, domestic production may be incentivized using laws that level the domestic playing field vis-à-vis foreign competition. Such laws restrict the importation of predatorily priced goods that threaten to displace domestic industry, and thereby give American industries the opportunity to grow and regain market share by operating in a fair economic environment. The trade laws include antidumping and countervailing duty laws; measures taken pursuant to Section 301 of the Trade Act of 1974, as amended; measures under Section 201 of the Trade Act of 1974, as amended; and restrictions under Section 232 of the Trade Expansion Act of 1962, as amended. Legal action taken under these authorities have been consistently upheld by U.S. Courts and the WTO, have been in use for decades, and are supported by substantial empirical data demonstrating their effectiveness.

Admittedly, lead time is always an important factor as domestic industrial growth does not happen overnight. As onshored production capacity gradually begins to come online (and/or as supply chains shift away from adversaries to trusted third-country partners), prohibitions on the use of high-risk hardware should be calibrated so as to not impede procurement for critical applications. Accordingly, the measures described above, including IEEPA and the trade laws, need not always be implemented in a sweeping manner. Whenever necessary, each prohibition on the use of foreign hardware may be phased in gradually to correspond with production capacity growth in both the domestic and allied markets. Beyond protecting U.S. systems from risks, these legal prohibitions

are also important in that they give investors confidence to support domestic projects with the knowledge that the project will be protected from economic predation in the future.

Finally, enforcement will be key. To the extent the U.S. Government prohibits the use of high-risk Chinese hardware in supply chains, it will need to ensure compliance. Today, most companies claim to lack adequate supply chain visibility at the third, fourth, fifth tier levels to comply with such restrictions. While this lack of visibility may be true, it is also deliberate. To be clear, companies have the ability to peer into their supply chains to eliminate prohibited hardware to ensure that they are compliant with any U.S. Government restrictions. The process involves a multi-level supply chain audit that begins with the product's bill of materials, and the audit only needs to be conducted for hardware items with potential for backdoor vulnerabilities. It does not need to reach every individual component in the finished item. Tamper-resistant products such as wires, chemicals, and plastics, are exempt from the audit trace, and by eliminating unnecessary traces, the audit process becomes focused, expeditious, and manageable for companies. The document contained in **Appendix Two** attached hereto represent a study I produced in cooperation with China Tech Threat that detail this audit approach. The document illustrates that compliance with prohibitions on the use of high-risk hardware is possible and not onerous. Inaction should no longer be an option.

In light of the ability to act immediately, the U.S. Government has no excuse for failing to act. The national security of the United States and the security and safety of United States persons depends on action now.

Appendix I

wiley

MEMORANDUM

DATE: October 20, 2023

RE: National Security Laws of the People's Republic of China and Their Capability to Undermine Compliance with U.S. or International Law

---

I. Introduction

The People's Republic of China (PRC) has spent over a decade shoring up a "legal Great Wall" to bolster national security protections and combat the ability of foreign regimes to undermine the government of China's (GOC), i.e., the Chinese Communist Party's (CCP), progress.[1] Several of the most prominent laws that have extraterritorial reach impacting Chinese, U.S., and foreign businesses, whether or not operating in China, are described below. Fundamentally, these Chinese laws conflict with U.S. laws and laws of other nations, and therefore render it impossible for businesses to simultaneously comply with both Chinese laws and the laws of the other jurisdictions in which they operate.

II. Biosecurity Law of 2020

The 2020 Biosecurity Law gives the National Security Commission of the CCP responsibility to coordinate biosecurity work.[2] The most prominent biosecurity area implemented to date is human genetic resources, reflected in Chapter VI of the law. The law's section on biotechnology states that the GOC must strengthen security management for research, development, and application activities and implement traceable management of "important equipment and special biological factors."[3] Biotechnology R&D efforts are categorized into high-, low-, and medium-risk activities under the law. Article 38 blocks foreign entities from conducting high- or medium-risk biotechnology R&D activities in China, requiring these entities to be "lawfully established and organized" as legal entities in the PRC and draft risk prevention and control plans.[4] Finally, the law imposes high penalties for violations. Under Article 75, the PRC can order a halt to R&D efforts while imposing a fine of up to 2 million RMB. Under Article 74, conduct found to be illegal

---

[1] China Daily, China builds legal Great Wall to safeguard national security: Official (Apr. 25, 2022), *available at* https://global.chinadaily.com.cn/a/202204/25/WS62663de4a310fd2b29e5926d.html.

[2] Zhonghua Renmin Gongheguo Shengwu Anquan Fa (中华人民共和国生物安全法) [Biosafety Law of the People's Republic of China] (promulgated at the 22nd Meeting of the Standing Comm. of the 13th Nat'l People's Cong., Oct. 17, 2020, effective Apr. 15, 2021), *translated in* China Law Translate, *Biosecurity Law of the P.R.C.*, https://www.chinalawtranslate.com/en/biosecurity-law/, Art. 4. ("Biosecurity Law").

[3] Biosecurity Law Art. 34, 39.

[4] Biosecurity Law Art. 38.

under the R&C provisions of the Biosecurity Law can result in sanctions on a company's managers and responsible personnel and management and fines between 1 and 10 million RMB where the value of unlawful gains is below 1 million RMB. When the value of unlawful gains is above 1 million RMB, fines can be between 10 and 20 million RMB and can be concurrently imposed with prohibition on conducting R&D efforts from 10 years to life.

While largely prompted to finalization by the COVID-19 outbreak, this law brings biosecurity into the umbrella of the national security apparatus, deeming it an "important aspect of national security."[5] Any individual or organization handling biological materials in China is potentially subject to the criminal provisions and penalties provided by the law. International biotechnology companies in a wide range of industries, including cosmetics, food and agriculture, healthcare, biotech, and pharmaceuticals, are affected by this law and its implementation. **The law has the effect of forcing companies working on R&D deemed as high- or medium-risk to incorporate as a PRC business entity and become subject to reporting requirements, potentially resulting in compulsory technology transfer in violation of U.S. laws.**

III. Negative Lists Updated in 2021 and 2022

The GOC restricts foreign investment through three negative lists. The Negative List for Market Access (Negative List) consists of sectors where investment from both Chinese and foreign companies is prohibited without special regulatory approval. Chinese and foreign investors are treated the same with respect to investment restrictions and approval requirements for sectors on the Negative List. The second, Special Administrative Measures for Foreign Investment Access (FDI Negative List), applies only to foreign investors. Similarly, the Special Administrative Measures for Foreign Investment Access in Free Trade Pilot Zones (FTZ Negative List) applies only to foreign investors with respect to their investment activities in free trade zones. The negative lists are updated regularly. The 2022 update to the Negative List added the news media sector to a list of 117 total items.[6] The current version of the FDI Negative List contains 31 industries, including mining of rare earths and tungsten, shipping and postal enterprises, legal businesses, research in the humanities and social sciences, and medical facilities.[7] The current version of the FTZ Negative List contains 27 of the industries listed on the FDI Negative list.[8] The four industries appearing on the FDI Negative List but not the FTZ Negative List are fishing of aquatic products, social research, printing of publications, and manufacture of Chinese proprietary medical products.

The GOC considers industries on the FDI Negative List to be critical to national security. For companies in FDI Negative List industries, Chinese government pre-approval is required for overseas initial public offerings. Overseas investors purchasing shares in overseas IPOs may not participate in the operation or management of these companies. The Administrative

---

[5] Biosecurity Law Art. 3.

[6] China Briefing, China's 2022 Negative List for Market Access (Apr. 12, 2022), *available at* https://www.china-briefing.com/news/chinas-2022-negative-list-for-market-access-restrictions-cut-financial-sector-opening/.

[7] C.I. Process, China foreign investment law and 2023 regulatory update (Aug. 8, 2023), *available at* https://www.ciprocess.com/china-foreign-investment-law-and-regulation.htm.

[8] Ziyou Maoyi Shiyan Qu Waishang Touzi Zhunru Tebie Guanli Cuoshi (Fumian Qingdan) (2021 Nian Ban) (自由贸易试验区外商投资准入特别管理措施（负面清单）（2021年版)) [Special Administrative Measures for Foreign Investment Access in Pilot Free Trade Zones (Negative List) (2021 Edition)] (promulgated by the 18th Executive Committee of the National Development and Reform Commission, Sept. 18, 2021, promulgated by Order No. 48 of the National Development and Reform Commission and the Ministry of Commerce, Dec. 27, 2021, effective, Jan. 1, 2021), *translated in* Garrigues, *Special Administrative Measures for Access of Foreign Investments in Pilot Free Trade Zones (Negative List) (2021 Edition)*, https://www.garrigues.com/sites/default/files/documents/2021_pftz_list.pdf.

Measures on Domestic Securities Investment by Qualified Foreign Institution Investors of 2012 provides that foreign investors may not participate in the operation or management of these companies and caps their holdings at 30% of shares. To avoid this equity cap, foreign investors that wish to participate in the market must enter partnerships, which often requires the transfer of technology, in addition to fraud, trade with sanctioned entities, and other types of activities that would be illegal under U.S. or international laws but entirely consistent with GOC laws.[9]

The PRC contends that the system of negative lists is comparable to review of investments in the United States by the Committee on Foreign Investment in the United State (CFIUS). These measures go beyond the scope of CFIUS review in the United States, however, by covering a broader range of transactions, including greenfield investments, and the review process is opaque. These negative lists generally foreclose certain investments entirely if foreign entities are unwilling to enter joint venture partnerships or incorporate as PRC entities.

IV. Hong Kong National Security Law of 2020

Article 3 of the law asserts that the GOC has "an overarching responsibility for national security affairs relating to the Hong Kong Specia Administrative region."[10] Article 54 specifies that the government will take "necessary measures to strengthen the management of" organs of foreign countries, international organizations, non-governmental organizations, and news agencies of foreign countries. This exposes U.S. citizens and companies to penalties and criminal fines for violations deemed a threat to Chinese national security, including calling for sanctions or authoring anti-GOC opinion articles. Under Article 55, courts in mainland China can exercise jurisdiction over national security cases that are "complex due to the involvement of a foreign country or external elements," in situations where the government in Hong Kong is unable to enforce the law, or if a "major and imminent threat to national security" has occurred.

V. Anti-Foreign Sanctions Law (AFSL) of 2021

The 2021 Anti-Foreign Sanctions Law (AFSL) provides legal basis for the GOC to implement retaliatory countermeasures against foreign laws and it prohibits compliance with foreign laws that undermine the GOC's or CCP's national objectives. In addition to creating a new PRC Countermeasure List, it codifies the administrative measures that created China's Provisions on the List of Unreliable Entities (PRC Entity List) and Measures for Blocking Importer Extraterritorial Application of Foreign Laws and Measures (Blocking Measures) – the GOC's mechanisms to sanction foreign persons or entities. Further, the AFSL creates a private right of action for Chinese citizens and organization to seek injunctive relief and damages against designated persons/entities.[11] The AFSL's first publicized use was in July 2021 when, in response to U.S. sanctions on PRC officials in Hong Kong, sanctions were imposed by China on seven U.S.

---

[9] U.S. Dep't of State, 2023 Investment Climate Statements: China, *available at* https://www.state.gov/reports/2023-investment-climate-statements/china/.

[10] Zhonghua Renmin Gongheguo Xianggang Tebie Xingzhengqu Weihu Guojia Anquan Fa (中华人民共和国香港特别行政区维护国家安全法) [Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region] (promulgated and effective at the 20th Meeting of the Standing Committee of the 13th National People's Cong., June 30, 2020, *translated in* Hong Kong Free Press, *In full: Official English translation of the Hong Kong national security law* (July 7, 202), https://hongkongfp.com/2020/07/01/in-full-english-translation-of-the-hong-kong-national-security-law/.

[11] Zhonghua Renmin Gongheguo Fan Waiguo Zhicai Fa (中华人民共和国反外国制裁法) [Anti-Foreign Sanctions Law of the People's Republic of China] (promulgated and enforced at the 29th Meeting of the Standing Comm. of the 13th Nat'l People's Cong., June 10, 2021), *translated in* China Law Translate, *Law of the PRC on Countering Foreign Sanctions*, https://www.chinalawtranslate.com/en/counteringforeignsanctions/#:~:text=Article%201%3A%20This%20Law%20is,our%20nation's%20citizens%20and%20organizations, Art. 12 ("AFSL").

persons, including former Commerce Secretary Wilbur Ross, the China director of Human Rights Watch, and directors and managers of the Congressional-Executive Commission on China and International Republican Institute.[12]

The GOC can designate persons and organizations to the PRC Countermeasure List that "directly or indirectly participate in the drafting, decision-making, or implementation"[13] of foreign sanctions. Relatives of designated persons, senior managers or actual controllers of listed organizations, organizations in which designated persons serve as senior management, and organizations in which designated persons are "actual controllers or participate in establishment and operations" may also be placed on the PRC Countermeasures List at the discretion of the GOC.[14] Entities on the PRC Countermeasures List can be subjected to visa restrictions, seizure and freezing of all types of property in the PRC, and prohibitions on any transactions or cooperation with organizations and persons in the PRC.[15] The law also includes an "{o}ther necessary measures" catch-all provision, which appears to give the GOC additional punitive authority.[16]

The ASFL is directly targeted towards U.S. sanctions, including primary sanctions imposed on Specifically Designated Nationals (SDNs) designated under the Uyghur Human Rights Policy Act of 2020 and the Hong Kong Autonomy Act of 2020 and secondary sanctions imposed on financial institutions transacting with SDNs. Because of its broad scope, the AFSL will cause challenges for MNCs operating in China because compliance with U.S. and other government sanctions will violate the AFSL and vice versa. The AFSL further expands the risk for both PRC and non-PRC companies and individuals who do business in China. Specifically, foreign investors or supply chain providers for Chinese technology companies will be impacted. The U.S. is not likely to accept compliance with the AFSL as a defense to alleged violations of U.S. sanctions. Potentially impacted companies can pursue mitigation measures including negotiating agreements to make litigation and arbitration subject to U.S. or international jurisdiction as the exclusive remedy from all disputes. Companies should also seek to include a provision in contracts that U.S. law governs, including in the event of a conflict of law, and avoid agreeing to contractual provisions permitting non-performance by parties based on the inclusion of a U.S. company or association with a person on the PRC Countermeasure List. Penalties should be included in contracts for breach even where failure to fulfill contract obligations is caused by the AFSL.

VI. Counter-Espionage Law of 2023

Updates to China's Counter-Espionage Law went into effect in July 2023. The PRC Ministry of State Security has emphasized the necessity of a system that makes it "normal" for the masses to participate in counter-espionage.[17] The law codifies this policy by obliging all PRC citizens and organizations to support and assist counter-espionage efforts.[18] However, the amendments to the law went beyond efforts to involve the populace: they expanded the scope of activities that can be considered espionage and codified the GOC's enforcement powers. Article 4(6) of the law

---

[12] Politico, Maeve Sheehey, China sanctions Wilbur Ross, others in response to U.S. warnings on Hong Kong (July 23, 2021), *available at* https://www.politico.com/news/2021/07/23/china-wilbur-ross-biden-us-warning-500686.

[13] AFSL Art. 4.

[14] AFSL Art. 5.

[15] AFSL Art. 6.

[16] AFSL Art. 6.

[17] Reuters, China wants to mobilise entire nation in counter-espionage (Aug. 1, 2023), *available at* https://www.reuters.com/world/china/china-wants-mobilise-entire-nation-counter-espionage-2023-08-01/.

[18] Zhonghua Renmin Gongheguo Fan Jiandie Fa (中华人民共和国反间谍法) [Counterespionage Law of the People's Republic of China] (promulgated at the 11th Meeting of the Standing Comm. of the 12th Nat'l People's Cong., Nov. 1, 2014, revised at the 2nd Meeting of the Standing Comm. of the 14th Nat'l People's Cong., Apr. 26, 2023), *translated in* China Aerospace Studies Institute, *In Their Own Words: Translation from Chinese source documents: Anti-espionage Law of the People's Republic of China*, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2023-05-15%20ITOW%20PRC%20Anti-Espionage%20Law.pdf, Art. 7-8 ("Counter-Espionage Law").

provides a new "other espionage activities" catch-all provision.[19] Further, where the prior law covered "state secrets and intelligence," Article 4(3) of the law expands the definition of espionage to cover "other documents, data, materials, or items related to national security" and information "incited, enticed, coerced, or bought" from state employees.[20] Article 4 also directly targets hacking and cyber-attacks, notably including disruption of "critical information infrastructure" in its list of acts of espionage and "agencies, organs, individuals, or other collaborators domestically or outside the PRC borders" within its espionage definition.[21]

The Counter-Espionage Law prompted the U.S. National Counterintelligence and Security Center, part of the Office of the Director of National Intelligence, to issue a public warning on heightened foreign business risk in China.[22] It has the potential to create legal risks and uncertainty for companies doing business in China because any documents, data, materials, or items could be considered relevant to PRC national security due to ambiguities in the law. The broad provisions of the law might apply to regular business activities. This law is of particular concern to companies doing business with the U.S. government, working on technology collaborations with Chinese enterprises, using data centers and cloud services in China, or conducting marketing research and business intelligence activities.[23] Such companies could be deemed to be conducting intelligence activities.

VII. Data Security Law of 2020

The Data Security Law broadly defines "Data Activities" in Article 2 to include activated undertaken by organizations and individuals outside of the PRC.[24] It imposes obligations in Article 28 to "promote economic and social development" in line with the CCP's "social morals and ethics."[25] Article 24 subjects companies processing "important data" to periodic security reviews.[26] Regardless of its origin, companies must obtain approval from the GOC under Article 36 to release data stored in China to any foreign judicial or law enforcement agencies.[27] The law authorizes CCP authorities to conduct compliance interviews.[28] Under Article 45, companies found in violation of regulations concerning "core data" can be penalized through forced shutdown of their businesses, fines of up to 10 million RMB, and criminal charges.[29] Under Article 48, companies found in violation of regulations concerning "important data" face penalties of up to 5 million RMB.[30] Article 26 authorizes the GOC to take reciprocal measures against "countries or regions" the CCP determines to be discriminatory with respect to data-related trade, investments, or technologies.[31]

---

[19] Counter-Espionage Law Art. 4(6).
[20] Counter-Espionage Law Art. 4(3).
[21] Counter-Espionage Law Art. 4(4).
[22] United States National Counterintelligence and Security Center, Safeguarding our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies (June 20, 2023), *available at* https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.
[23] Forbes, Jill Goldenziel, China's Anti-Espionage Law Raises Foreign Business Risk (July 3, 2023), *available at* https://www.forbes.com/sites/jillgoldenziel/2023/07/03/chinas-anti-espionage-law-raises-foreign-business-risk/?sh=73989abc769e.
[24] Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated at the 29th Meeting of the Standing Committee of the 13th National People's Cong., June 10, 2021, effective, Sept. 1, 2021.), *translated in* DIGICHINA, *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ Art. 2 (Data Security Law).
[25] Data Security Law Art. 28.
[26] Data Security Law Art. 24
[27] Data Security Law Art. 36.
[28] *Id.*
[29] Data Security Law Art. 45.
[30] Data Security Law Art. Art. 48.
[31] Data Security Law Art. 26.

The U.S. Department of Homeland Security indicates that this law represents a shift in the CCP's attitude away from protecting Chinese data systems as a defensive mechanism and towards collecting data as an offensive act.[32] Given the Data Security Law's expansive compliance obligations, companies doing business in China must seek advice before exporting data from the PRC. The broad language in Article 2 extending liability beyond the territory of the PRC is a political tool in the U.S.-China technology relationship. Further, Article 24 gives the CCP the power to respond if CFIUS were to alt an acquisition over data access, or if any government enacts restrictions based on data issues related to China. It targets the expansion of CFIUS jurisdiction in 2018 to review transactions involving sensitive U.S. data, responding to U.S. government efforts to restrict companies like TikTok from storing data abroad.

VIII. Network Product Security Vulnerability Reporting Law of 2021

The Network Product Security Vulnerability Reporting Law imposes strict reporting requirements and controls on publicization of network security information. Article 4 direct organizations and individuals not to "illegally collect, sell, or publish" information on network product security vulnerabilities.[33] Article 7(2) mandates reporting to the PRC Ministry of Information and Technology on network security vulnerabilities within 2 days of discovery.[34] Organizations and individuals engaged in network product security work are directed by Article 9(3) not to "carry out malicious sensationalization" of vulnerabilities.[35] Article 9(6) specifies that during periods when the GOC holds "major activities," these organizations and individuals are prohibited from publishing information on network product security vulnerabilities without the consent of the Ministry of Public Security.[36] Further, Article 9(7) provides that information on vulnerabilities that is not public "must not be provided to overseas organizations or individuals other than the network product provider."[37] Penalties are provided for in accordance with the PRC's Cybersecurity Law.

The law tightens controls on the flow of information to the public, particularly before vulnerabilities have been resolved or addressed by the Ministry of Information and Technology and Ministry of Public Security. The law and its ambiguity in its references to covered entities, including individuals who discover product vulnerabilities, complicates the business environment for companies and vendors of network devices.

IX. Personal Information Protection Law of 2021

Like the Data Security Law and AFSL, the Personal Information Protection Law (PIPL) imposes extraterritorial jurisdiction. Article 3 of the law specifies that it applies that it is applicable not only

---

[32] U.S. Dep't of Homeland Security, Off. of Trade and Economic Security, Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China at 7 (Dec. 22, 2020), *available at* https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[33] Gongye he xinxihua bu Guojia hulianwang xinxi bangongshi Gong'anbu guanyu yinfa wangluo chanpin anquan loudong guanli guiding de tongzhi (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知) [Notice from the Ministry of Industry and Information Technology, the State Internet Information Office, and the Ministry of Public Security on the issuance of regulations for the management of network product security vulnerabilities] (promulgated by Order No. 66 of the Ministry of Industry and Information Technology, National Internet Information Office, Ministry of Public Security, July 12, 2021, effective, Sept. 1, 2021), *translated in* China Law Translate, *Provisions on the Management of Network Product Security Vulnerabilities* (July 14, 2021), https://www.chinalawtranslate.com/en/product-security-vulnerabilites/#:~:text=Provisions%20on%20the%20Management%20of%20Network%20Product%20Security%20Vulnerabilities,-By%20China%20Law&text=Article%201%3A%20These%20Provisions%20are,to%20defend%20against%20security%20risks Art. 4 (Network Product Security Vulnerability Reporting Law).

[34] Network Product Security Vulnerability Reporting Law Art. 7(2).

[35] Network Product Security Vulnerability Reporting Law Art. Art. 9(3).

[36] Network Product Security Vulnerability Reporting Law Art. Art. 9(7).

[37] Network Product Security Vulnerability Reporting Law Art. 9(7).

to organizations and individuals who process personally identifiable information (PII) in China, but also and organizations and individuals who process data of Chinese citizens' PII outside of China.[38] Article 3 also includes a catchall provision applying the law to "other circumstances provided in laws or administrative regulations."[39] Article 36 expands the restrictions imposed by the Data Security Law by requiring companies operating in the PRC to locally store all personal information collected and produced.[40] Non-PRC companies that need to provide PII to entities outside the PRC are required to agree to a GOC-formulated contract.[41] Article 38 mandates a security assessment by GOC authorities for cross-border transfers of personal information.[42] However, Article 38 references Article 40, specifying that if laws, administrative regulations, GOC information department provisions prevail if they prohibit such a security assessment.[43] "Personal Information" is broadly defined in Article 4 as "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons," including video, voice, or image data.[44] Article 66 provides penalties for violating the law including fines of up to 50 million RMB or 5% of a company's annual revenue for the previous year, suspension of related business activities, revocation of operating permits for recertification, and negative social credit scores.[45] Directly responsible persons can be prohibited from holding supervisory positions or serving as personal information protection officers for an unspecified period of time and fined up to 1 million RMB.[46]

Like the Data Security Law, the PIPL would create conflicts of law that delay or impede discovery requests from U.S. and international courts. It focuses on protecting individuals, society, and national security in the CCP's political system, mirroring the broad political aims of the GOC.

X. Foreign Relations Law of 2023

This law, which provided a comprehensive framework for PRC foreign relations for the first time, is the latest in a sequence of statutes targeting U.S. and other countries' export control and sanctions regimes. The broadly scoped Foreign Relations Law asserts in Article 8 that "any organizations or individuals" that violate it and any other relevant laws will be held liable.[47] Article 32 asserts the PRC's right to employ countermeasures or restrictive measures that threaten its "sovereignty, security, and developmental interests."[48] This provision echoes language in the AFSL, reaffirming the GOC's ability to provide responses to foreign sanctions and emphasizing its authority to take action. Article 32 of the Foreign Relations Law likewise states that the PRC

---

[38] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Committee of the 13th National People's Cong., Aug. 20, 2021, effective, Nov. 1, 2021), *translated in* DIGICHINA, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ Art. 3 (PIPL).

[39] *Id.*

[40] PIPL Art. 6.

[41] *Id.*

[42] PIPL Art. 38.

[43] PIPL Art. 38, 40.

[44] PIPL Art. 4.

[45] PIPL Art. 66.

[46] *Id.*

[47] Zhonghua Renmin Gongheguo Duiwai Guanxi Fa (中华人民共和国对外关系法) [The Law on Foreign Relations of the People's Republic of China] (promulgated by the Third Meeting of the Standing Comm. of the 14th Nat'l People's Cong., June 28, 2023, effective July 1, 2023), t*ranslated in* China Law Translate, *Foreign Relations Law (2023)* (June 28, 2023), https://www.chinalawtranslate.com/en/foreign-relations-law/, Art. 8 ("Foreign Relations Law").

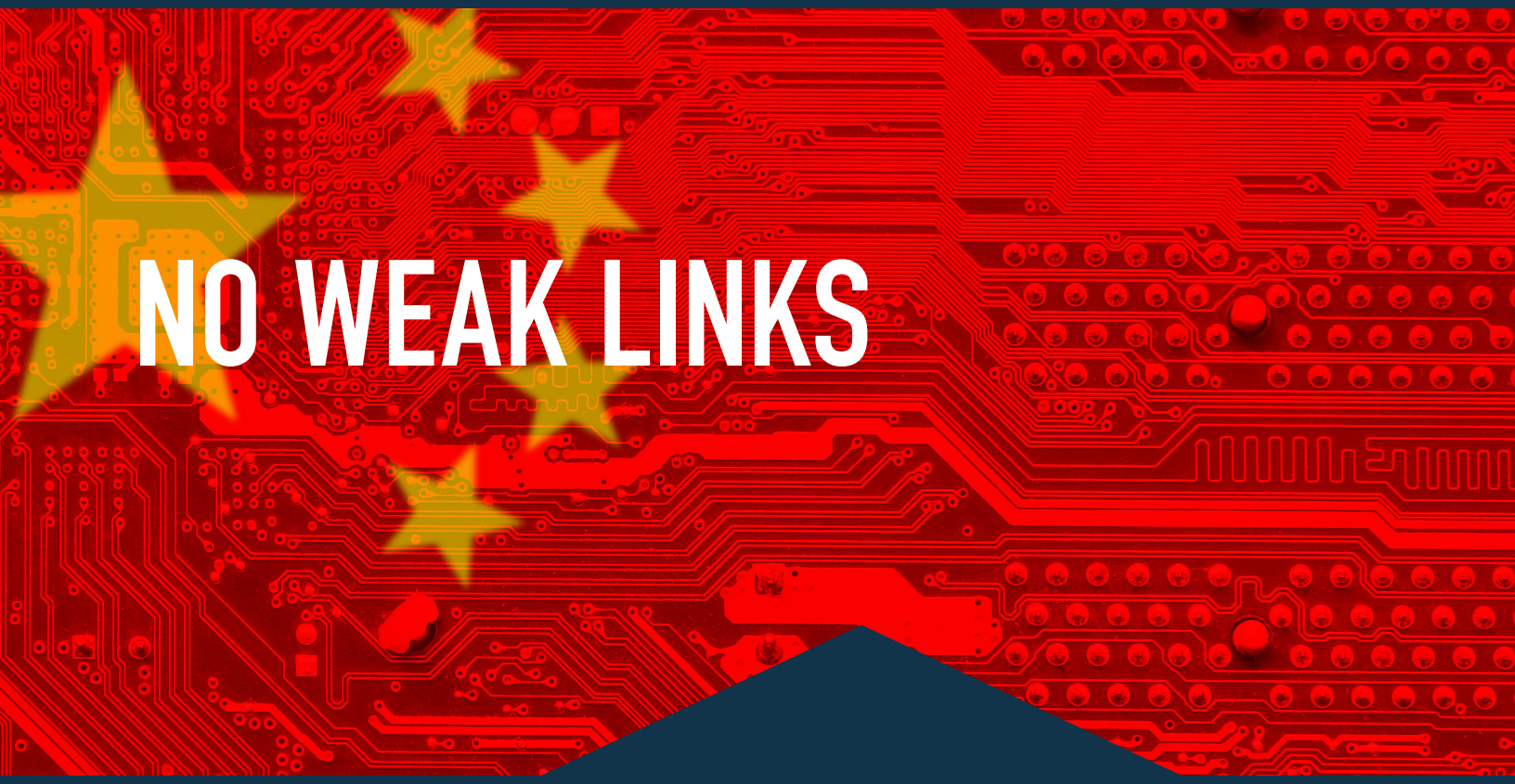
[48] Foreign Relations Law Art. 32.

will act to strengthen the implementation and application of laws and regulations in "foreign-related fields," suggesting wider extraterritorial application of the laws discussed above.[49]

Coupled with others, including the ASFL and the Data Security Law, the Foreign Relations Law demonstrates the PRC's continued efforts to assert its authority over companies and individuals doing business in China and abroad. It further codifies the PRC's intent to apply its national security laws extraterritorially in conflict with other countries' national security laws. Companies caught between conflicting laws will be forced to weigh their options and take risk-based approaches to their activities.

[49] Foreign Relations Law Art. 32.

Appendix II



NO WEAK LINKS

A STRATEGY FOR KEEPING U.S. DEFENSE SUPPLY CHAINS CLEAN OF DANGEROUS CHINESE TECHNOLOGIES

JUNE 1, 2023

IN CONSULTATION WITH NAZAK NIKAKHTAR, CHINA TECH THREAT SPECIAL ADVISOR[1]

China TECH THREAT

TABLE OF CONTENTS

PREFACE: WHY THE U.S. GOVERNMENT NEEDS TO ENSURE "CLEAN" SUPPLY CHAINS FOR DOD AND OTHER AGENCIES

The United States Government controls troves of sensitive information. Agencies responsible for American defense, intelligence, and diplomatic efforts, as well as numerous other federal agencies, rely on billions of dollars' worth of technologies to protect that information. Keeping that information secure is always a challenge, as the recent case of alleged leaker Jack Teixeira, a Massachusetts Air National Guardsman, indicates. Foreign adversaries' attempts to penetrate U.S. systems can have equally or even more damaging consequences.

Unfortunately, major government contractors may unwittingly be compromising sensitive information in their reliance on on electronic technology and/or software manufactured by companies owned or controlled by foreign adversaries, especially China. Today many items used by the federal government – e.g. smartphones, batteries, vehicles, and weapons systems – contain components with backdoor surveillance capabilities that retrieve sensitive U.S. Government information, "kill switches" that enable a foreign adversary to disable equipment while in use or tamper with the device remotely, causing systems disruptions or intentional malfunction. The additional reality is that a substantial quantity of these foreign-sourced components come from the People's Republic of China (PRC).

FBI Director Christopher Wray says that there is "no country that presents a broader threat" than the People's Republic of China.[2] At the same time, China is both a major technology manufacturer and home to a 2017 intelligence law which compels Chinese companies and citizens to turn over to the Chinese government any information it deems necessary for national security purposes. While Chinese business leaders have said they would refuse government directives, independent analysts insist they would be forced to comply.

> "They have no position to say no to the Chinese government."[3]
>
> *- Dr. Miles Yu, former State Department China Policy Advisor, commenting on the obligations of Chinese companies under Chinese law*

So why would contractors rely on suspect technology and how could our adversaries use backdoors? In recent years, Chinese President Xi Jinping has directed tens of billions of dollars in investments into semiconductor national champions YMTC, SMIC, and CXMT, growing their market share by 30 percent.[4] These sizable investments, coupled with China's non-market economy structure where prices of goods, land, electricity, and labor are intentionally distorted by the central government, enable Chinese products to be priced lower than competitors by approximately 40%-60% in many instances. But these price discrepancies are artificial (not driven by market forces), and are always subject to manipulation by the Chinese government. Nevertheless, major American contractors working with the U.S. Government have opted over the past 15 years to rely on Chinese electronics equipment and software, largely because Chinese products are less expensive.

It is technologically conceivable that the Chinese government could tamper with certain products in ways that would put U.S. national security interests in serious peril.[5] One prominent weapons system used on Ukrainian battlefields is BAE Systems' AGM88 harm air-to-surface missile.[6] This weapon relies on an array of highly sophisticated semiconductors. What if it was built with semiconductors from PRC-controlled companies and the PRC manipulated the microchips to disable the weapons?

While there are a handful of U.S. Government procurement regulations that prohibit the acquisition of Chinese equipment, the regulations are not fully enforced. Government contractors also lack adequate visibility into their upstream supply chains to ensure their own compliance. The U.S. Government has itself acknowledged many times that it lacks full visibility into its own supply chain dependence on Chinese entities. This creates a serious vulnerability in both the security of its electronics communications systems and its military systems.

The U.S. government does not know the extent to which Chinese technologies have penetrated the defense supply chain. This lack of visibility can and should be cured, and the process of doing so is not prohibitively complex. The solution depends on (1) knowing which critical government systems may rely on insecure technology and (2) replacing the technology with items sourced from trusted suppliers.

PROBLEM STATEMENT: CONTRACTORS' OPAQUE SUPPLY CHAINS INVITE INFILTRATION

Present high-technology supply chains are extremely layered. Federal government vendors, contractors, and "primes" (original equipment manufacturers) often lack adequate visibility into the supply chains of their second tier, third tier, etc. suppliers of goods or software. This lack of visibility encourages supply chain infiltration by foreign adversaries. Such risk to U.S. Government systems is unacceptable: infiltration into the Government's information and communications technology and services ("ICTS") systems and defense systems can introduce surveillance and/or hardware malfunction capabilities that could compromise America's communications, intelligence, and weapons capabilities and put the Defense Department's warfighters in serious peril. These vulnerabilities could impact allies as well, to the extent they procure U.S. equipment and software, and vice versa.

The core problem with existing supply chain rules is that they require self-policing without any enforcement mechanism.

At present, some, albeit limited, U.S. Government authorities exist that discourage or outrightly prohibit reliance on materials sourced from certain Chinese entities. These include the Federal Acquisition Regulations, the Defense Federal Acquisition Regulations Supplement, the Consolidated Appropriations Act of 2018, Section 889 of the 2019 National Defense Authorization Act ("NDAA") and Section 5949 of the 2023 NDAA. The core problem with these rules is that they require contractors to self-police, which most (if not all) simply lack the will (but not the resources) to do.[7] Nor does the U.S. Government have a mechanism to enforce these prohibitions, which means that vendors routinely ignore these requirements. The risks associated with ignoring supply chain vulnerabilities are too great and the Government's mitigation strategy needs to evolve

SOLUTION: INFORMATION GATHERING AND U.S. GOVERNMENT REPORTING THROUGH DEFENSE PRODUCTION ACT SURVEYS

Despite U.S. Government inaction to date, the Government does have authority to compel vendors to review their supply chain vulnerabilities and report them to the Government. For example, the Pentagon can mandate its primes to audit their supply chains for risks. Pursuant to authorities under section 705 of the Defense Production Act of 1950 as amended ("DPA") (50 U.S.C. app. 2155) and § 104 of Executive Order 13603 of March 16, 2012 (National Defense Resources Preparedness, 77 FR 16651, 3 CFR, 2012 Comp., p. 225), the U.S. Government conducts studies to determine whether the U.S. industrial base's capabilities appropriately support the U.S. Government, defense sector, or the broader domestic commercial supply chain.

To produce these studies, the Government (through the Department of Commerce) may issue Defense Production Act Surveys to collect detailed information related to the health and competitiveness of the U.S. industrial base from Government sources and private individuals or organizations. Such surveys are mandatory (they operate analogous to subpoenas) and are routinely issued to assess specific weak links in supply chains. Unfortunately, to date, the Surveys have not been used to comprehensively probe the supply chains of vendors that provide critical ICTS and defense capabilities to the U.S. Government. This is a significant shortcoming. The U.S. government has the capabilities to identify the source of the technological components in its supply chains. It should use them.

SURVEY METHODOLOGY AND OUTPUT: The following describes how the U.S. Government, including the Pentagon, could compel contractors and defense primes to audit their supply chains. The end goal would be for these contractors/primes to (1) certify that the chains are clean from components/software sourced from entities associated with foreign countries of concern or (2) report to the Government the presence of problematic components/software in their supply chains. Entities associated with foreign countries of concern would be entities located in or affiliated with (through ultimate beneficial owners, "UBOs") foreign countries of concern (including but not limited to China and Russia) – hereinafter collectively referred to as Foreign Entities of Concern, i.e., "FEOCs." The audit steps are straightforward and could materially affect the U.S. Government's supply chains for the better.

The Commerce Department, which would administer the Surveys, would start with a pilot project that could then be replicated for the broader industrial base, as follows:

1. COMMERCE DEPARTMENT ISSUES SURVEYS TO CONTRACTORS

Commerce would develop and issue on behalf of federal agencies surveys to all U.S. Government contractors/primes within a specific sector, for example unmanned aerial systems. (UAS). The

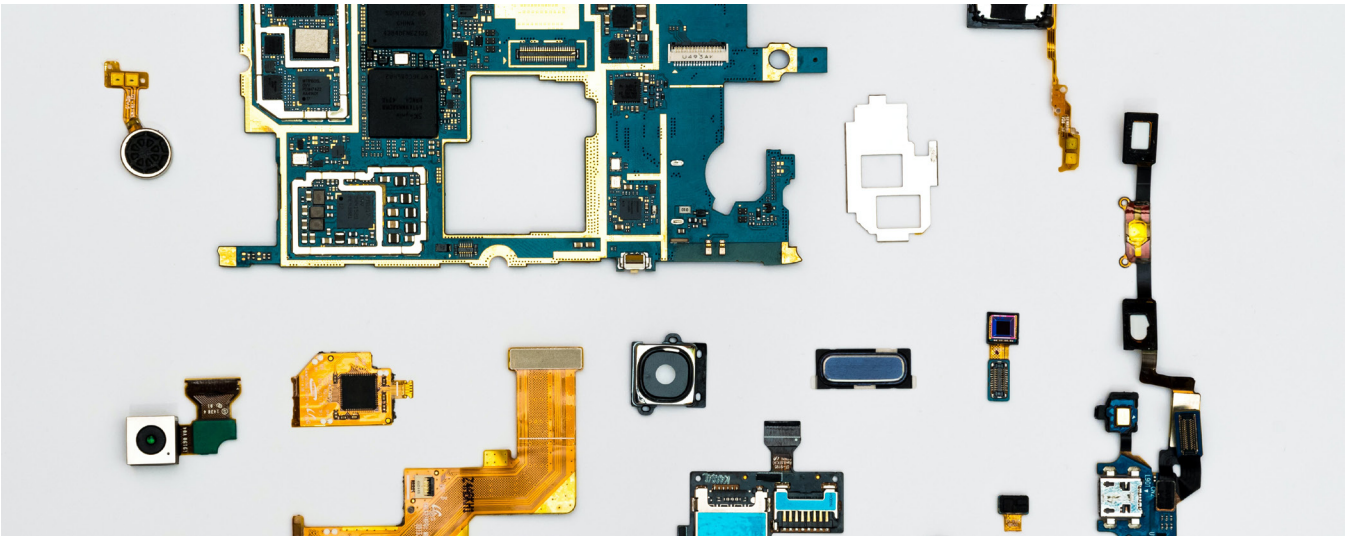
surveys would request information from the contractors/primes as to their material and software supply chains, and then require the contractors/primes to identify any potential critical components/software sourced from FEOCs. The following information would specifically be required:

a. All bills of materials ("BOMs") required to produce the final product (e.g., UAS) and imbedded critical components (e.g., lithium-ion batteries).

b. All software bills of materials ("SBOMs") required to produce the imbedded software.[8]

c. Description of all critical components/software included in the BOMs/SBOMs sourced from FEOCs. Critical components/software are all parts of the final product that could be used by a foreign adversary to (1) damage the operations of the final product, (2) create safety risks, (3) collect and transmit surveillance-type data from or through the final product or any related component/software, and (4) cause any other harm to U.S. national security.

d. Certification from the contractor/prime that it has conducted a complete audit of its supply chains up to the critical components/software, and that it confirms the absence of critical components/software from FEOCs, or if such supply chain vulnerabilities exist such that a certification cannot be provided, the contractor/prime would be required to report the supply chain vulnerability to the U.S. Government.



2. SURVEY RECIPIENTS CONDUCT DUE DILIGENCE

Upon receipt of the surveys, contractors/primes would need to take the following steps to comply with requirements 1.a-d:

a. Obtain the requested BOMs and SBOMs from in-house engineers and additional BOMs/SBOMs from all parts/software suppliers.

b. Identify all critical components from the BOMs/SBOMs identified in 2.a.

c. Steps 2.a and 2.b would continue until the contractor/prime has obtained BOMs/SBOMs identifying every upstream input used to manufacture the critical components that make up its final product (e.g., UAS). An upstream input would be defined as a product derived from

raw materials which are commodities and do not require specialized engineering processes to manufacture or which are tamper-resistant in their final form. So, for a lithium-ion battery, the inputs of interest would include the anode, cathode, electrolyte, and all building blocks of any embedded software code.

d. The contractor/prime would then identify all critical components that could be used to maliciously interfere with the operation of the final product, its parts, or otherwise collect surveillance data as described in 1.c above.

3. CONTRACTORS DIRECT SUPPLY CHAIN AUDITS

Based on the steps listed in 2.a-d above, the contractor/prime would then be required to conduct audits of its supply chains up to its critical component/software suppliers. This is a straightforward process and requires standard audit-type checks that identify all critical component/software suppliers to ensure that they are trusted. This is accomplished through a process of:

a. inventory record checks and production schedules,

b. examinations of supplier contracts,

c. purchase order reviews,

d. sales invoice reviews, and

e. corroboration against relevant accounting legers.

With respect to the UBO of each critical component/software supplier, there are databases, such as Dun & Bradstreet, that provide ownership information. To the extent a contractor/prime is unable to find the UBO of any supplier, this gap should be reported to the U.S. Government.

PROCESS EXAMPLE: THE LITHIUM-ION BATTERY

To illustrate the simplicity of this process, we provide the example of a lithium-ion battery included in a UAS, where the lithium-ion battery is produced by a battery pack manufacturer (tier two), who sources lithium-ion cells from cell suppliers (tier three), who then source the raw material anodes, cathodes, and electrolytes from other suppliers (tier four). Because the anodes, cathodes, and electrolytes are tamper-resistant, the supply chain audit would stop after the identities of the cell manufacturers are known (i.e., tier three being the highest point in the supply chain where tampering could occur).

In this example, the UAS contractor/prime could audit its own production records as well as the production records of its lithium-ion battery pack manufacturer (or it could contract with a third-party auditor to do this). To begin, the UAS manufacturer would examine its BOMs to determine the specific type of lithium-ion batteries that it incorporated into the UASs sold to the U.S. Departments of Interior and Defense. Using the BOMs, the UAS manufacturer would then identify the unique, product-specific serial numbers associated with the batteries to identify the battery pack manufacturers. The next steps involve supply chain audits of the battery pack manufacturers. Using the same serial numbers plus relevant production/sales records, the battery pack manufacturers will be able to identify their cell providers for each battery pack produced and sold to the contractor/prime. Relevant production/sales records include those listed in 3.a-e above. Again, the lithium-ion battery supply chain trace would end at the lithium-ion cell producer because the cell producer's raw materials are tamper-resistant, meaning that the highest level in the supply chain where malicious vulnerabilities could be introduced is at the cell level. If the cell and battery pack manufacturers are non-FEOCs, then the battery supply chain check is complete and the audit is successful.

The battery's SBOM, as it is itself a nested inventory (i.e., a self-contained list of ingredients that make up software components), could itself be checked by the UAS manufacturer. Alternatively, there are firms that can review software codes to detect backdoors and potentially malicious code, and could be hired by contractor/primes to review software that is being used.

CONCLUSION: A SUCCESSFUL PILOT PROGRAM PAVES THE WAY FOR BROADER IMPLEMENTATION

The foregoing audit checks may take several weeks up to several months to complete (depending on the complexity of the supply chain). However, even for larger contractors/primes, such as aircraft manufacturers, the traces can be accomplished within a year.[9]

Again, audit results and certifications should be provided to the U.S. Government through Survey responses, and records should be kept for at least five years. Certifications should confirm the absence of any components/software provided by FEOCs. Should contractors/primes find that certain components/software were provided by FEOCs, disclosures should be provided to the U.S. Government through Survey responses, and the Government should take immediate remedial action.

This pilot project, when proven to be successful, could be extended to all U.S. government contractors/primes using the same methodology described here.

ENDNOTES

1 China Tech Threat staff drafted this paper after consulting with CTT Advisor Nazak Nikakhtar. From 2018 to 2021, Nikakhtar served as the Department of Commerce's Assistant Secretary for Industry & Analysis at the International Trade Administration (ITA). Nikakhtar also fulfilled the duties of the Under Secretary for Industry and Security at Commerce's Bureau of Industry and Security (BIS). Additionally, Nikakhtar spearheaded the United States' first-ever whole-of-government initiative to evaluate and strengthen supply chains across all strategic sectors of the economy.

2 https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122

3 https://www.youtube.com/watch?v=jk3u2sfPQAg

4 https://www.nytimes.com/2022/08/29/technology/china-semiconductors-technology.html

5 https://semiengineering.com/chip-backdoors-assessing-the-threat/

6 https://www.reuters.com/graphics/UKRAINE-CRISIS/ARMS/lgvdkoygnpo/

7 This would be much like the current self-policing prohibitions on the importation and use of items derived from forced labor or conflict minerals.

8 SBOM is "a list of all the open source and third-party components present in a codebase. An SBOM also lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks." https://www.synopsys.com/blogs/software-security/software-bill-of-materials-bom/

9 Audits may be conducted every few years depending on the nature of the contractor's/prime's operations. If, however, the contractor/prime is required by the U.S. Government to keep FEOC components/software out of its supply chains and establish a robust system to ensure ongoing compliance, then audits will not need to be conducted as frequently.

NO WEAK LINKS

A STRATEGY FOR KEEPING U.S. SUPPLY CHAINS CLEAN OF DANGEROUS CHINESE TECHNOLOGIES

IN CONSULTATION WITH NAZAK NIKAKHTAR, CHINA TECH THREAT SPECIAL ADVISOR

www.chinatechthreat.com