Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "Current and Emerging Technologies in U.S.-China Economic and National Security Competition"

Jack Corrigan
Senior Research Analyst
Center for Security and Emerging Technology (CSET), Georgetown University
February 1, 2024

Co-chairs Wessel and Helberg, distinguished commissioners and staff, thank you for the opportunity to participate in today's hearing. It is an honor to testify alongside the experts on this panel and the two panels later in the day. I am currently a senior research analyst at the Center for Security and Emerging Technology at Georgetown University, where I study the U.S. innovation ecosystem, the flow of domestic and international tech talent, and U.S.-China technology competition.

Today my testimony will focus on the last topic, and specifically U.S. policies related to the procurement of Chinese-manufactured information and communications technology and services (ICTS). For more than a decade, U.S. leaders have warned that ICTS produced by certain Chinese companies presents national security risks. In recent years, policymakers have enacted a variety of measures intended to purge this technology from U.S. digital networks and supply chains. These measures (which I refer to broadly as "procurement bans") grant policymakers the authorities necessary to restrict the use of technologies deemed to present national security risks ("designated ICTS") across U.S. digital networks. While federal and state government agencies have slowly started to implement these procurement bans, there remain economic and bureaucratic factors that could impede the effectiveness of these policies.

My testimony will 1) provide a brief overview of the various risks posed by designated Chinese ICTS; 2) detail existing regulations related to foreign ICTS procurement; 3) discuss the prevalence of designated Chinese ICTS in the United States and barriers to implementing effective procurement bans; and 4) conclude with recommendations for how policymakers can begin developing a more targeted and cohesive nationwide framework for regulating Americans' use of foreign ICTS. These four recommendations include:

- Prioritizing broad, flexible federal authorities
- Fully funding "rip and replace" programs and related measures
- Targeting procurement bans to high-risk sectors, networks, and use cases
- Monitoring the implementation and effectiveness of procurement bans

Understanding the Risks Posed by Designated Chinese ICTS

Policymakers have long expressed concerns that ICTS produced by certain Chinese technology companies could pose significant risks to national security.[1] Their apprehension has grown over the last decade as the Chinese Communist Party (CCP) enacted measures that more closely linked the Chinese private sector to the government's intelligence operations. For instance, China's 2017 National Intelligence Law mandated that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."[2]

While there are numerous specific concerns regarding the use of Chinese ICTS in U.S. digital networks, for the purposes of this hearing, we can think of these risks as falling into two broad categories: cybersecurity risks and economic risks.

Cybersecurity Risks

For years, national security leaders have warned that certain types of Chinese ICTS may contain backdoors or other vulnerabilities that could allow Chinese actors to gain unauthorized access to critical U.S. networks, platforms, and data. Technologies compromised in this way could potentially function as conduits for various Chinese actors to conduct espionage, cyberattacks, and other nefarious activities on users' networks. There is evidence that the CCP has indeed used Chinese-manufactured technology to conduct intelligence operations abroad. In 2019, the CCP was accused of using Huawei equipment to spy on the headquarters of the African Union.[3] An FBI investigation also revealed that Huawei equipment deployed near military bases in the United States was "capable of capturing and disrupting highly restricted Defense Department communications," although investigators did not disclose any evidence that such breaches had occurred.[4]

While federal policymakers seem generally aware of the cybersecurity risks posed by certain types of Chinese ICTS, the extent to which state and local government officials and commercial organizations recognize these risks remains unclear.[5] Only a handful of states have enacted policies to restrict the purchase of designated ICTS from China and other countries, and virtually no local governments have done so. While many government officials may be aware of the risks these technologies pose on an abstract level, in many cases their agencies lack the in-house technical expertise to fully assess and address those risks within their networks.

It is important to note that the actual risks posed by designated Chinese ICTS are highly context dependent. Integrating a piece of compromised equipment into the network of a military base presents very different risks to national security than using that same piece of equipment at an elementary school in rural Illinois, for example. To date, discussions of the cybersecurity risks posed by designated Chinese ICTS have largely ignored this distinction. Moreover, it is worth noting that Chinese-manufactured ICTS is not the only avenue through which Chinese actors

could gain unauthorized access to U.S. digital networks. The last decade has provided numerous examples of security breaches involving ICTS produced by U.S. companies. In 2023, for instance, Chinese actors exploited a vulnerability in Microsoft Outlook to access email accounts at the U.S. State and Commerce departments, as well as dozens of other U.S. organizations.[6] Clarifying the specific threats Chinese-manufactured ICTS pose in different contexts would help policymakers craft more targeted procurement bans and avoid placing undue financial burdens on public and private organizations.[7]

Economic Risks

The Chinese technology companies that have faced scrutiny on national security grounds have generally been market leaders. In 2018, the year U.S. policymakers began cracking down on the domestic proliferation of certain types of Chinese ICTS, Huawei was the top provider of telecommunications equipment and the second largest smartphone producer in the world.[8] Even today, Hikvision and Dahua, which have also been subject to U.S. procurement bans, remain the world's top two providers of digital surveillance equipment by revenue.[9] In many cases, firms achieved this market dominance with the help of Chinese industrial policy measures, which enabled companies to expand their global reach and offer lower prices than competitors headquartered in the United States and U.S.-allied countries.[10] This affordability has made certain types of Chinese ICTS popular among U.S. consumers, particularly those who make purchasing decisions primarily based on cost (such as financially constrained state and local governments). These buyers often cannot afford to pay higher prices for alternatives to designated Chinese ICTS. For example, a rural school district may find itself in a situation where it must decide between using a Hikvision or Dahua security camera to monitor a school playground or going without security cameras altogether.[11] Even in situations where consumers are aware of the cybersecurity risks posed by these technologies, they may determine that vulnerable equipment is better than no equipment.

On the whole, these economic dynamics have created a situation in which many consumers in the United States and allied countries rely almost entirely on Chinese companies for access to key technologies. The persistent demand for cheap ICTS has helped Chinese technology companies to entrench their market position and made it more difficult for non-Chinese competitors, whose products are often higher quality but more expensive, to achieve economies of scale that could ultimately drive down prices.

U.S. Policies on Chinese ICTS

To date, U.S. policies related to the procurement and use of Chinese ICTS have focused almost exclusively on mitigating cybersecurity risks rather than addressing economic risks of dependency on Chinese technology. These measures largely involve blocking various public and

private U.S. entities from integrating certain foreign ICTS ("covered ICTS") into their networks and authorizing certain U.S. government bodies to develop and implement procurement bans. While existing policies provide the policymakers with the authorities necessary to regulate the procurement, those authorities have not always been implemented effectively. Here I provide an overview of the major policies policymakers have enacted to mitigate the risks posed by certain types of Chinese ICTS:

Section 889 of the 2019 National Defense Authorization Act (2018)

Section 889 prohibits federal agencies from:

1. Using ICTS produced by five Chinese companies deemed to pose national security risks: Huawei (华为), ZTE (中兴通讯), Hikvision (海康威视), Dahua (大华), and Hytera (海能达);
2. Working with contractors that use covered ICTS anywhere in their networks; and
3. Awarding grants or loans to any entity for the purchase of covered ICTS.[12]

The potential impact of Section 889 is significant, as it would eliminate covered ICTS from the networks of federal agencies and the tens of thousands of companies with whom they do business. However, given the breadth of the federal contracting ecosystem and the ubiquity of certain types of covered ICTS, agencies may lack the capacity to enforce the law, which could limit its effectiveness.[13]

SECURE Technology Act (2018)

Title 2 of the SECURE Technology Act authorizes federal agencies to withhold contracts from vendors whose technologies present national security risks and creates the interagency Federal Acquisition Security Council (FASC) to evaluate those risks and implement mitigation strategies.[14] Those mitigation strategies may include exclusion orders (banning future procurement of covered ICTS) or removal orders (directing agencies to purge covered ICTS from their networks). The FASC has not yet issued any such orders. However, as of December 4, 2023, federal contractors are required to check for new FASC orders on SAM.gov.[15] This recent development indicates the FASC may soon begin to exercise its authorities.

Commerce ICTS Rule (2019)

The ICTS Rule authorizes the Commerce Department to restrict the purchase and use of foreign ICTS by any U.S. person (individual, business, government, etc.).[16] Specifically, the authority allows the department to block or unwind certain ICTS transactions that:

1. Pose "undue or unacceptable" national security risks, and
2. Involve U.S. persons and designated "foreign adversaries."*

The Commerce Department will consider more than a dozen criteria when determining whether to prohibit certain ICTS transactions and offer interested entities the opportunity to contest those determinations.[17] While no such rulings have been issued to date, the Bureau of Industry and Security (BIS) stood up an Office of Information and Communications Technology and Service (OICTS) to implement the rule and is reportedly conducting an investigation into the Russian security firm Kaspersky Lab.[18]

Secure and Trusted Communications Networks Act (2020)

The Secure and Trusted Communications Networks Act, enacted in 2020, authorized the Federal Communications Commission (FCC) to create a list of companies that pose "unacceptable" national security risks.[19] Organizations that receive FCC funds—a group that includes hundreds of public and private entities—are prohibited from buying ICTS from firms on the list. The law also created a program (the Secure and Trusted Communications Networks Reimbursement Program) through which small U.S. telecom providers could receive funding to "rip and replace" covered ICTS already deployed in their networks.† Though promising, the program currently faces a major budget shortfall.[20] Additional funding from Congress is required to support an effective rip and replace initiative.

FCC Equipment Authorization (2022)

In November 2022, the FCC voted to block new equipment authorizations for ICTS produced by the five Chinese firms listed in Section 889 (i.e., Huawei, ZTE, Hikvision, Dahua, Hytera).[21] The decision effectively outlaws the import, sale, and use of this covered ICTS across the United States, marking a significant step toward removing technology deemed to present national security risks from U.S. digital networks. However, the measure will take time to achieve its desired effect. The ban only applies to new authorizations, meaning products from Huawei and other companies that have already received FCC authorization can still be legally bought and sold in the United States. The FCC is reportedly exploring how restoring its net neutrality regulations might impact its authorities to purge designated ICTS from U.S. networks.[22]

State Procurement Bans (2019 – Present)

* Executive Order 13873, from which the ICTS Rule originated, explicitly names China, Russia, Iran, North Korea, Cuba, and Venezuela as foreign adversaries.

† The program is initially focused on replacing equipment from Huawei and ZTE.

Over the years, a handful of state governments have also enacted measures to restrict the procurement of foreign ICTS deemed to present national security risks.[23] However, the scope and effectiveness of these procurement bans vary widely. While some states have aligned their regulations with federal procurement bans, others have attempted to create their own procurement blacklists. These custom lists often target different companies than the federal regulations and are, in some cases, too broad to be meaningfully enforced.[24] Some state regulations also focus on prohibited vendors rather than prohibited technology, which creates major loopholes that allow covered ICTS into government networks.[25]

Final Thoughts on ICTS Procurement Authorities

Today, U.S. policymakers possess the authorities necessary to eliminate Chinese ICTS deemed to present national security threats from U.S. networks. However, these authorities have not always been implemented effectively and, given the overlap between various authorities, the current regulatory landscape can often be difficult to navigate. Going forward, policymakers should work to build a more targeted and cohesive nationwide framework for regulating the use of designated Chinese ICTS. This framework would rely on federal orders—namely those issued through the FASC and OICTS—to govern the use of Chinese ICTS across the private and public sector. The FCC could also play a critical role in supporting efforts to replace the designated ICTS already deployed in U.S. networks if provided more funding for its existing rip and replace program. I will offer more details on how this framework could be implemented in the final section of this testimony.

The Challenges of Eliminating Designated Chinese ICTS from U.S. Digital Networks

Despite the aforementioned policies and discourse highlighting the risks posed by certain types of Chinese ICTS, these technologies are still prevalent across the United States. A study from the Center for Security and Emerging Technology (CSET) found that between 2015 and 2021, at least 1,681 U.S. state and local government entities purchased equipment produced by the five companies listed in Section 889, and while these transactions decreased after federal bans went into effect, they did not stop altogether.[26] The CSET analysis should be viewed as a low-end estimate of the number of state and local governments using this equipment—the actual number is likely much higher.

To be clear, these transactions, by and large, were perfectly legal. Few state governments and virtually no local governments have implemented procurement bans on Chinese ICTS, and federal policymakers have not yet used the authorities at their disposal (ICTS Rule) to regulate state and local governments' procurement behavior. At the federal level, there is no evidence to suggest wide-scale use of designated Chinese ICTS. However, these technologies remain popular in the commercial sector due to their relatively low cost.

There are a number of factors that help explain why the country's existing regulatory framework has not been wholly effective in removing designated Chinese ICTS from U.S. digital networks. These include:

Supply Chain Complexity

The ICTS supply chain includes tens of thousands of companies scattered across the globe. ICTS produced by Chinese firms designated as national security risks may be sold under different names and brands, or they may be integrated into products and services from otherwise trustworthy suppliers.[27] In a few isolated cases, federal agencies have reportedly purchased covered Chinese ICTS that was sold under different brand names.[28] ICTS is also often sold through third-party vendors, who may further obscure the technologies' origin. This complexity makes it difficult to determine the provenance of a particular piece of equipment, which in turn complicates the process of identifying and excluding particular types of ICTS from untrustworthy sources.

Incohesive Policy Strategy

Today, U.S. policy towards Chinese ICTS consists of a patchwork of overlapping, complicated regulations. In this environment, it is not always clear to organizations which rules and regulations they ought to follow. Developing a more cohesive regulatory framework—and communicating those policies clearly—will allow businesses, governments, and other organizations to make informed ICTS procurement decisions. Given its broad jurisdiction and unique intelligence capabilities, the federal government is in the best position to lead this effort. The regulations implemented through the FASC and OICTS can serve as the backbone for this policy framework. Aggregating and publishing orders issued by these bodies in a publicly available "master list" of federal regulations on foreign ICTS procurement would further clarity on legal obligations and best practices for different public and private organizations.

Slow Implementation

While federal policymakers have the necessary authorities for keeping designated foreign ICTS out of U.S. digital networks, many of their most powerful authorities have yet not been used. The FASC, for instance, has not issued a single order to block or remove designated ICTS from government networks. The Commerce Department's OICTS, which has the authority to regulate all public and private ICTS transactions, has also not issued any rulings or decisions. To some extent, these delays are understandable—foreign technology procurement bans are a relatively new type of regulation, and implementing them effectively takes time and resources. These regulations have proven to be legally contentious, so it is important that the processes and

procedures involved in their implementation are transparent, fair, and airtight.[29] However, without FASC or OICTS orders to block the procurement of designated ICTS, this technology will continue to proliferate across U.S. digital networks.

Looking to the future, even after government bodies begin issuing orders, enforcing those regulations will likely prove challenging. The domestic ICTS market is expansive, touching virtually every person, commercial business, and government agency in the United States. As such, providing staff, funding, and other resources to support effective oversight will be critical to the successful implementation of these policies. Without such a commitment, we will see potentially risky technologies and services continue to proliferate across the U.S. digital networks.

Underfunded Rip and Replace Programs

Purging designated Chinese ICTS from U.S. digital networks is a resource-intensive endeavor. These high costs make it unlikely that organizations will be able to undertake rip and replace efforts without the financial support of the government. Today, the FCC's rip and replace program faces a budget shortfall of roughly $3.1 billion, and that funding gap will only grow if the program expands to cover Chinese ICTS beyond Huawei and ZTE. Providing additional funds for rip and replace programs will be critical to ensuring their effectiveness.[30]

The High Costs and Ambiguous Benefits of Procurement Bans

Procurement bans can impose significant costs, and for a lot of organizations, the benefits of complying with these regulations are not always clear. As previously noted, there are often few alternatives to designated Chinese ICTS available at comparable prices. As such, forgoing cheap Chinese technology often drives up procurement costs to levels that many organizations cannot afford. Insufficient funding for existing rip and replace programs, as well as proactive funding for future ICTS procurement initiatives, has only exacerbated this problem.

Furthermore, while paying more for increased security is justifiable for some organizations (government agencies, critical infrastructure operators, etc.) for others, the costs of such measures likely outweigh their benefits. Overall, the risks associated with specific types of foreign ICTS vary widely based on how and where that technology is deployed. Banning these technologies may not be warranted in situations where security breaches present few potential national security risks. Analyzing the costs and benefits of procurement bans in light of the full threat landscape is crucial for ensuring government resources are efficiently distributed and regulations on foreign ICTS procurement target the sectors, networks, and use cases where the risks to national security are highest.

Looking Ahead

Addressing the risks posed by certain types of Chinese ICTS will require a targeted and cohesive nationwide policy framework on foreign technology procurement. The federal government is well-positioned to develop and implement this framework, and policymakers already have the necessary authorities to do so. Going forward, agencies should seek to design procurement bans that target the sectors, networks, and use cases where breaches present the greatest risks to national security and ensure these regulations do not impose unnecessary compliance costs on businesses, government agencies, and other organizations. Striking this balance will be critical for successfully mitigating the risks posed by designated foreign ICTS. To conclude, I offer four recommendations for policymakers looking to design such a framework:

1. Prioritize broad, flexible federal authorities

The federal government is well-positioned to lead the development of a nationwide regulatory framework for the purchase and use of foreign ICTS. Agencies have various policy levers they can use to keep designated ICTS out of U.S. digital networks, but the FASC process and ICTS Rule are the most promising and should be prioritized in the years ahead. If implemented effectively, these two authorities could govern ICTS procurement across every economic sector: the FASC process would allow federal agencies to keep designated technology out of their networks, and the ICTS Rule would enable the Commerce Department to regulate ICTS deployed across the networks of non-federal entities (state and local governments, commercial businesses, etc.). These two authorities also offer policymakers the flexibility to tailor bans to particular applications of particular technologies (e.g. outlawing certain Chinese-manufactured surveillance cameras on the networks of financial institutions) and update regulations as the threat landscape changes.[‡] Existing federal procurement bans could eventually be incorporated into these two frameworks (e.g. OICTS could issue orders prohibiting U.S. telecom companies from using ICTS from the entities on the FCC covered list). Once successfully implemented, the FASC process and ICTS Rule could eliminate the need for other procurement bans.

Additionally, orders issued by the FASC and OICTS should be aggregated and published in a publicly available "master list" of federal regulations on foreign ICTS procurement. This list could be modeled on the Treasury Department's "Sanctions List Search" portal.[31] Publishing these orders in an accessible, easy-to-search online format would make it easier for other public and private entities to keep track of the regulations they must follow and better understand the landscape of foreign ICTS risks. This list could also serve as a baseline for any organization that wishes to implement its own restrictions on foreign ICTS procurement.

---

‡ Procurement bans that enshrine designated companies in federal statute, like Section 889, are less flexible than these executive branch authorities.

2. **Fully fund "rip and replace" programs and related measures**

Rip and replace programs will play a critical role in keeping designated foreign technology out of U.S. digital networks. Replacing this equipment is a costly endeavor, and organizations are unlikely to undertake these efforts without financial support. Ensuring programs like FCC's Secure and Trusted Communications Networks Reimbursement Program are fully funded would ensure businesses, government agencies, and other organizations have the resources to comply with relevant procurement bans. As new regulations go into effect, these programs could be expanded to offset the higher procurement costs that certain resource-constrained entities will face as they transition away from covered ICTS.

3. **Target procurement bans to high-risk sectors, networks, and use cases**

Eliminating all designated Chinese ICTS from every U.S. network would be prohibitively expensive, if not impossible. Furthermore, overly broad bans (such as those enacted by some state governments) can impose enormous costs across the economy, particularly when there are few cost-competitive alternatives from trusted sources. As such, it is crucial that policymakers target procurement bans and rip and replace funding at the sectors, networks, and use cases where breaches present the greatest risks to national security. The intelligence community, Cybersecurity and Infrastructure Security Agency, and other federal bodies can inform these decisions on how to target bans so as to maximize their impact and avoid imposing undue compliance costs.

4. **Monitor the implementation and effectiveness of procurement bans**

Finally, as new procurement bans are enacted, OICTS and other agencies should collect data to monitor the implementation and effectiveness of their regulations across different sectors, geographies, and ICTS categories. This information would help inform policymakers on how to proceed with future regulations and highlight ways to make existing regulations more effective. This monitoring capability would likely require additional staff, funding, and resources, which could be allocated by Congress.

---

[1] Mike Rogers and Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," (U.S. House of Representatives, October 8, 2012), 3, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf#page=11.

[2] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[3] Salem Solomon, "After Allegations of Spying, African Union Renews Huawei Alliance," Voice of America News, June 6, 2019, https://www.voanews.com/a/after-allegations-of-spying-african-union-renews-huawei-alliance/4947968.html.

[4] Katie Bo Lillis, "CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt U.S. nuclear arsenal communications," CNN, July 25, 2022, https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.
[5] Jack Corrigan, Sergio Fontanez, and Michael Kratsios, "Banned in D.C." (Center for Security and Emerging Technology, 2022), https://cset.georgetown.edu/wp-content/uploads/CSET-Banned-in-D.C.-1.pdf#page=11.
[6] Raphael Satter and Zeba Siddiqui, "Chinese hackers stole emails from US State Dept in Microsoft Breach, Senate staffer says," *Reuters*, September 27, 2023, https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/.
[7] Corrigan et al., "Banned in D.C."
[8] "Key Takeaways – Worldwide Telecom Equipment Market 2018" Dell'Oro Group, March 4, 2019, https://www.delloro.com/telecom-equipment-market-2018-2/; Jeb Su, "Huawei Fortifies #2 Spot in Global Smartphone Market, Beating Apple Again," Forbes, November 2, 2018, https://www.forbes.com/sites/jeanbaptiste/2018/11/02/huawei-fortifies-2-spot-in-global-smartphone-market-beating-apple-again/?sh=541020fd1305.
[9] "2023 Security 50 Industry Report," *ASMag.com*, Accessed January 2024, https://www.asmag.com//2023_security50_industry_report.pdf.
[10] Kim Sutter, "Made in China 2025" Industrial Policies: Issues for Congress (Washington, DC, Congressional Research Service, 2020), https://sgp.fas.org/crs/row/IF10964.pdf; Alex Rubin, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi, "The Huawei Moment" (Center for Security and Emerging Technology, 2021), https://cset.georgetown.edu/publication/the-huawei-moment/.
[11] Corrigan et al., "Banned in D.C."
[12] Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, Pub. L. No. 115-232, 132 Stat. 1917 (2018).
[13] Corrigan et al., "Banned in D.C."
[14] Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, 132 Stat. 5178 (2018).
[15] FAR 4.2303 (2024).
[16] Securing the Information and Communications Technology and Services Supply Chain, 86 FR 4909 (2021).
[17] Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications, 88 Fed. Reg. 39353-39358 (June 16, 2023), https://www.federalregister.gov/documents/2023/06/16/2023-12925/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software
[18] John D. McKinnon and Dustin Volz, "Biden Administration Weighs Action Against Russian Cybersecurity Firm," *The Wall Street Journal,* April 7, 2023, https://www.wsj.com/articles/biden-administration-weighs-action-against-russian-cybersecurity-firm-b84afcd7; "Office of Information and Communications Technology and Services (OICTS)," *BIS.gov*, Accessed January 2024, https://www.bis.doc.gov/index.php/oicts.
[19] Today, the FCC's covered list includes 10 companies: the five Chinese firms covered by Section 889, four other telecommunications companies with direct or indirect ties to the CCP, and Kaspersky Lab. For more, see: Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020).
[20] Linda Hardesty, "FCC approves some Huawei rip and replace extensions, sends letter to Congress," *Fierce Wireless*, October 13, 2023, https://www.fiercewireless.com/wireless/fcc-approves-some-huawei-rip-and-replace-extensions-sends-letter-congress.
[21] Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, 37 FCC Rcd 13493 (2022).
[22] David Shepardson, "FCC says it could boost authority over Huawei, ZTE equipment," *Reuters*, September 28, 2023, https://www.reuters.com/business/media-telecom/us-telecom-board-says-it-could-boost-authority-over-huawei-zte-equipment-2023-09-28/.
[23] Corrigan et al., "Banned in D.C."
[24] Ibid.
[25] Ibid.
[26] This includes the five Chinese companies identified in Section 889 (Huawei, ZTE, Hikvision, Dahua, and Hytera Communications). See: Corrigan et al., "Banned in D.C."
[27] In most cases, OEM relationships are not intended to deceive customers or mask the provenance of a particular product, but rather to create market synergies. For example, most of the personal computers sold by Dell use chips produced by Intel, graphics cards produced by NVIDIA, and software (Windows)

produced by Microsoft. In this case, Intel, NVIDIA, and Microsoft are all OEMs.

[28] Zack Whittaker, "US government agencies bought Chinese surveillance tech despite federal ban," TechCrunch, December 1, 2021, https://techcrunch.com/2021/12/01/federal-lorex-surveillance-ban/.

[29] For instance, the federal government engaged in a protracted legal battle with the Russian cybersecurity firm Kaspersky Lab after the Department of Homeland Security (DHS) banned the company's products from federal networks. Kaspersky alleged that DHS violated the company's constitutional rights by issuing a ban before giving it a chance to defend itself, among other things. The current FASC and OICTS processes attempt to avoid this issue, requiring policymakers to justify their actions against particular vendors and giving companies the chance to appeal. For more information on the Kaspersky ban, see: Joseph Marks, "DHS, Kaspersky Resume Court Battle Over Government Ban," Nextgov, February 6, 2018, https://www.nextgov.com/cybersecurity/2018/02/dhs-kaspersky-resume-court-battle-over-government-ban/145774/; Aaron Boyd, "U.S. Finalizes Rule Banning Kaspersky Products From Government Contracts," Nextgov, September 9, 2021, https://www.nextgov.com/cybersecurity/2019/09/us-finalizes-rule-banning-kaspersky-products-government-contracts/159742/.

[30] Hardesty, "FCC approves some Huawei rip and replace extensions, sends letter to Congress."

[31] "Sanctions Search List," Office of Foreign Assets Control, accessed October 2022, https://sanctionssearch.ofac.treas.gov/.