Issue Brief

# Banned in D.C.

## Examining Government Approaches to Foreign Technology Threats

**Authors**
Jack Corrigan
Sergio Fontanez
Michael Kratsios

CSET CENTER for SECURITY and EMERGING TECHNOLOGY

October 2022

## Executive Summary

For nearly a decade, U.S. national security leaders have warned that information and communications technology and services (ICTS) produced by Huawei, ZTE, and other Chinese companies may serve as conduits for government espionage and other nefarious activities. In response, policymakers have sought to purge this untrustworthy technology from U.S. supply chains.

Over the last five years, the federal government has enacted a series of measures regulating the purchase of foreign ICTS on the grounds of national security, including:

- **Section 889 of the 2019 National Defense Authorization Act,** which prohibited federal agencies from using equipment and services from five Chinese tech companies and working with contractors that use covered equipment.
- **Title 2 of the SECURE Technology Act**, which created a federal council to analyze supply chain security threats and recommended orders to remove or exclude certain technologies from federal networks.
- The **ICTS rule**, which allows the U.S. Department of Commerce to block public and private procurement and use of certain foreign ICTS.
- The **Secure and Trusted Communications Networks Act**, which permitted the Federal Communications Commission (FCC) to restrict the purchase of certain ICTS using federal funds.

These measures aimed to provide federal policymakers with the authorities to identify and remove untrustworthy ICTS from critical federal networks and—where possible and appropriate—from critical networks owned and operated by state, local, and private sector entities. However, these authorities are still relatively new, and it remains to be seen whether they will be effectively scoped and implemented.

Defending U.S. networks against untrustworthy foreign ICTS also requires buy-in from state and local policymakers, but to date, they have largely not revised their procurement laws to address those threats. Only five states—Florida, Georgia, Louisiana, Texas, and Vermont—have enacted measures to limit the procurement of foreign ICTS on national security grounds, and some of these existing policies contain loopholes that would allow untrustworthy technology to slip into government networks. All the while, public officials have continued integrating untrustworthy technologies into schools, hospitals, prisons, public transit systems, and government offices around the country. Our analysis of public government procurement records provided by GovSpend found that at least 1,681 state and local entities purchased

equipment and services prohibited at the federal level under Section 889 between 2015 and 2021.

Keeping untrustworthy foreign technology out of government networks requires a more harmonized effort across all levels of government. Given its resources and intelligence capabilities, the federal government must spearhead this effort. Under the SECURE Technology Act, government leaders can tailor federal procurement prohibitions for different environments and applications. By providing the Commerce Department with the funds and staff to implement the ICTS rule—through a sanctions-based model—they can work to keep untrustworthy technology out of state, local, and critical private networks. Using these two authorities, policymakers can maintain effective procurement prohibitions that will remain current with the changing threat landscape. FCC regulators can further protect U.S. networks by blocking authorizations of untrustworthy technology.

Given their resource constraints and limited mandate, state and local governments should not be expected to independently grapple with the national security implications of foreign ICTS. However, by adhering to federal rules on foreign ICTS procurement, state and local governments can protect their digital infrastructure and keep procurement practices up to date without constant regulatory, administrative, or legislative interventions. This may entail following mandatory ICTS rule restrictions or, if the rule is not implemented effectively, enacting policies that prevent the use of ICTS prohibited by federal agencies. Federal policymakers can further enable state and local governments to address foreign technology threats by creating a master list of foreign ICTS covered by procurement prohibitions, strengthening existing information sharing channels, and increasing funding for rip and replace programs.

## Table of Contents

## Introduction

On the morning of December 1, 2018, Meng Wanzhou stepped off a plane at Vancouver International Airport. She expected a short layover before catching a flight to Mexico City, but before making the transfer, Meng was intercepted by Canadian border security officers. After hours of questioning, she was officially apprehended under a U.S. warrant. Meng, the chief financial officer of the Chinese telecommunications giant Huawei Technologies, would spend the next 33 months under house arrest facing extradition to the United States.[1] Though she was ostensibly arrested on charges of financial fraud, the incident came in the midst of the U.S. government's intensifying pressure on Huawei, whose CEO and founder Ren Zhengfei also happened to be Meng's father.

For years, policymakers had expressed concerns that, given the Chinese government's broad control over commercial entities, Chinese technology companies could pose significant national security risks. In 2012, the U.S. House of Representatives Permanent Select Committee on Intelligence warned that industry giants like Huawei and ZTE provided Chinese intelligence apparatus "a wealth of opportunities . . . to insert malicious hardware or software implants into critical telecommunications components and systems."[2] This apprehension was reinforced in subsequent years as the Chinese government enacted a series of measures to strengthen the ties between the private sector and the state. The efforts culminated in the 2017 National Intelligence Law, which mandated that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."[3]

By the time of Meng's arrest, fears about the security threats posed by Chinese ICTS had reached a fever pitch. In late 2017, Congress barred the U.S. Department of Defense (DOD) from using information and communications technology and services (ICTS) provided by Huawei and ZTE in certain critical systems, including those involved in missile defense and nuclear command and control.[4] FBI Director Christopher Wray warned lawmakers in 2018 that Huawei and ZTE provided the Chinese Communist Party (CCP) with "the capacity to exert pressure or control over our telecommunications infrastructure . . . the capacity to maliciously modify or steal information, and . . . the capacity to conduct industrial espionage."[5] Soon after, the DOD pulled Huawei and ZTE mobile phones and modems from stores on military bases, and the Federal Communications Commission (FCC) issued a proposal to cut off funding to domestic telecom providers that use equipment and services from companies that "pos[e] a national security threat," citing Huawei and ZTE.[6]

These measures signaled a growing awareness among U.S. leaders that foreign governments could weaponize the global technology supply chain, and China's central position in that network offered the CCP a dangerous amount of leverage.[7] At the time, Huawei was the world's top provider of telecommunications equipment and second largest smartphone producer.[8] The global surveillance industry was—and still is—dominated by a pair of Chinese firms, Hangzhou Hikvision Digital Technology and Dahua Technology.[9] Chinese companies also held major positions in the markets for drones, mobile radios, and other technologies.

For U.S. national security leaders, the broad reach of these firms—and their integration into the networks of the United States and its allies—presented major national security and economic threats. If the CCP wanted to use the Chinese tech industry as a conduit for espionage and other nefarious activities, it could potentially gain access to all these global networks. Even if firms were not weaponized in this way, their growing market power threatens the global dominance of competitors in the United States and U.S.-allied countries. Some Chinese firms, like Huawei, commanded markets with no viable U.S. competitors in the first place. China's efforts to increase its global economic competitiveness were paying off, and U.S. leaders feared the country could fall behind in 5G, artificial intelligence, and other emerging industries.

In light of these threats, U.S. policymakers sought to purge the supply chain of equipment from certain foreign technology companies. Doing so required the creation of a new regulatory regime. While the government had systems for regulating the export of goods and services as well as foreign investment in the United States, there was no mechanism for controlling inbound goods and services.

In the subsequent years, policymakers implemented a series of measures to prevent compromised technology from entering U.S. networks, including:

- **Section 889 of the 2019 National Defense Authorization Act (NDAA)**, which prohibited federal agencies from using equipment and services from five Chinese tech companies and working with contractors that use covered equipment.[10]
- **Title 2 of the SECURE Technology Act**, which created a federal council to analyze supply chain security threats and recommended orders to remove or exclude certain technologies from federal networks.[11]
- The **ICTS rule**, which gave the U.S. Department of Commerce broad authority to review and block purchases of certain equipment and services across the public and private sector.[12]

- The **Secure and Trusted Communications Networks Act**, which prohibited FCC funds from being used to buy certain foreign ICTS and created a program to fund the replacement of those technologies.[13]

Collectively, these measures are intended to form a shield that protects the United States against the threats posed by covered ICTS.* While these policies overlap and intersect in different cases, each serves a distinct purpose, enabling national security leaders to tailor procurement prohibitions to meet the needs of different types of organizations.

However, the federal government cannot unilaterally defend U.S. networks against foreign technology threats. A wide variety of public services and critical infrastructure systems are managed by state and local governments, and thus far, these entities have generally not revised their procurement laws to address those threats.† Only a handful of states have restricted purchases of foreign technologies that pose security threats. Generally, these existing measures are poorly targeted, and some contain loopholes that would allow covered ICTS to slip into government networks. Procurement records show that in recent years thousands of state and local entities have deployed covered ICTS in schools, hospitals, prisons, public transit systems, and government offices around the country. If the ultimate goal is to keep untrustworthy foreign technology out of U.S. networks (particularly those associated with government agencies and critical infrastructure), a more harmonized and comprehensive framework is needed across every level of government, with federal policymakers leading the way.

In this brief, we begin with a discussion of the potential threats posed by foreign technology and the challenges of removing covered ICTS from government supply chains. We then survey the landscape of federal and state regulations around foreign technology procurement, as well as the extent to which covered ICTS has made its way into state and local government networks. We conclude with five recommendations for constructing a more cohesive framework for defending U.S. networks against foreign technology threats.

---

* Throughout this paper, the phrase "covered ICTS" refers to technology products and services from foreign companies that federal agencies and other U.S. entities are restricted from buying.

† Many critical infrastructure systems are also owned and operated by private entities, and keeping untrustworthy foreign ICTS out of these systems is also critical to national security. Today, federal agencies work closely with these operators to manage supply chain risks. For more, see: "Critical Infrastructure Sectors," *U.S. Cybersecurity and Infrastructure Security Agency*, accessed October 2022, https://www.cisa.gov/critical-infrastructure-sectors.

## Defining Foreign Technology Threats

Understanding the specific risks posed by foreign ICTS is critical to effectively assessing government responses to those threats. For the purposes of this brief, we can think of these threats as falling into three broad categories: **backdoors**, **human vulnerabilities**, and **economic risks**.

To date, most proponents of foreign ICTS procurement bans have justified their position on the grounds that covered technologies could contain secret **backdoors**, or vulnerabilities that are deliberately baked into the technologies. These hidden bugs can be exploited by adversaries to spy, disrupt, or conduct other nefarious activities on users' networks. In recent years, U.S. policymakers emphasized the threat of potential backdoors to garner support for their crackdown on Chinese technology companies like Huawei. Under China's national security regulations, they argued, the CCP could order private firms to embed backdoors in their products, turning them into conduits for government espionage. As such, federal agencies needed to eliminate these technologies from their supply chains.

Evidence suggests that the CCP has indeed exploited Chinese ICTS to conduct surveillance abroad. Huawei equipment was implicated in a years-long espionage operation that involved Chinese spies exfiltrating data from the African Union headquarters, as well as efforts to restrict access to internet content in dozens of countries.[14] FBI investigators also found that Huawei equipment installed near U.S. military bases could be used to disrupt or intercept critical DOD communications, and security researchers have also uncovered vulnerabilities in ICTS manufactured by Huawei, Hikvision, and other foreign companies.[15] However, it is unclear whether those vulnerabilities represent backdoors installed at the government's behest or run-of-the-mill software bugs that bad actors have exploited. No technology is perfectly secure, and Chinese hackers have repeatedly proven their ability to compromise government networks using existing vulnerabilities.[16] These more conventional breaches are in many cases easier to orchestrate than supply chain attacks involving backdoors, and they carry fewer potential economic costs as well.*

Still, foreign technologies can pose other hazards, such as **human vulnerabilities**. Most hardware and software must be serviced over the course of its life cycle, and the technicians who perform replacements, upgrades, and other maintenance may find

* The global backlash that firms would face if they were discovered building backdoors into products might disincentivize them—and their national governments—from pursuing this path.

themselves in positions with broad access to users' networks. Should those individuals be compromised by a foreign adversary, they could potentially install malware, exfiltrate data, or conduct other nefarious activities on their behalf. Without the proper safeguards in place, any organization that uses foreign ICTS is exposed to these operational security risks.

In the international context, foreign technologies can also pose **economic risks**. Countries benefit both economically and geopolitically when their domestic companies become more globally competitive. The Chinese government has long viewed economic security as a critical component of national security, using industrial policy and other mechanisms to position domestic companies at key nodes in the global supply chain.[17] As Chinese companies gain market share, the United States and its allies may find themselves relying on their biggest geopolitical competitor for access to key technologies.

## Challenges of Procurement Prohibitions

Purging a particular product from any supply chain is a difficult feat. The global technology market is vast, complex, and opaque, which makes it exceedingly difficult for governments to understand the provenance of the products they purchase.

The modern ICTS supply chain spans tens of thousands of companies scattered across the globe, and the links between these firms are not always clear. Equipment manufactured by one firm may contain components sourced from many different suppliers, and it might be sold under the brand name of yet another company.

For instance, cameras manufactured by Dahua Technology, the Chinese surveillance company, are sold under the Dahua brand and also under the names of subsidiaries like Canada-based Lorex. Dahua also serves as the "original equipment manufacturer" for dozens of other vendors, selling them products that are then repackaged and sold under the purchaser's brand.

These types of arrangements—which are common across the tech industry—make it difficult for governments, private companies, and other consumers to determine exactly whose equipment and services they are buying.[18] Furthermore, much of the technology that ends up on government networks is purchased through third-party vendors and integrators, adding yet another layer of complexity to the supply chain. Some distributors have continued doing business with Chinese companies that federal leaders have identified as national security risks, which makes weeding their products out of government supply chains harder still.[19]

Even if they understand their supply chains, government agencies face other challenges when attempting to purge covered ICTS from their networks.

One major obstacle is that procurement bans can increase the cost of acquiring equipment. Chinese ICTS is generally cheaper than equivalent products from non-Chinese companies, making it an appealing option for cash-strapped government agencies.[20] A basic Hikvision dome camera retails for about $90, while similar cameras made by firms in Canada, Japan, and South Korea sell for more than double the price.[21] Therefore, prohibiting the use of this cheaper Chinese equipment and forcing government agencies to buy costlier but trustworthy alternatives drives up IT expenses. Costs are even higher if agencies are required to rip and replace the covered ICTS that already resides in their networks.[22]

These challenges are compounded by the lack of public information on the threats posed by foreign technology. Though national security leaders frequently discuss the general risks posed by equipment from Huawei and other companies, they rarely offer details on specific vulnerabilities or breaches attributed to particular products.* Given this lack of clarity, state and local policymakers may hesitate to devote energy, resources, and political capital to removing untrustworthy tech.

Many government entities also lack the in-house technical expertise and procedures to understand and address such threats in the first place, and those that do may prioritize addressing immediate threats like ransomware over the more abstract risks posed by foreign ICTS.[23] We will discuss in a later section how government agencies that lack this expertise are more likely to make procurement decisions based primarily on cost rather than security.

Lastly, depending on their structure, procurement bans can disincentivize vendors from doing business with government agencies. For instance, Section 889 prohibits federal agencies from awarding contracts to contractors that use covered ICTS even if that equipment is not involved in performing the contract. Thus, the measure effectively acts as a procurement prohibition for both federal agencies and federal contractors. Given the costs of following this regulation, companies that do not already sell to the federal government may be unwilling or unable to do so.

Despite these challenges, it is critical that governments at all levels work to eliminate untrustworthy technologies from their supply chains. In the following sections, we will discuss the steps that the federal government has taken to secure the ICTS supply chain, the landscape of state-level procurement bans, and the extent to which state and local governments have introduced untrustworthy ICTS into their networks.

* Backdoors have indeed been uncovered in products manufactured by Huawei, ZTE, Hikvision, and other companies, but it remains unclear whether those vulnerabilities were exploited by the Chinese government, at least publicly. For more, see: "Hikvision Backdoor Exploit," IPVM, September 3, 2017, https://ipvm.com/reports/hik-exploit; Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," The Wall Street Journal, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256; Michael Lee, "Backdoor Found in ZTE Android Phone, ZDN.net, May 14, 2012, https://www.zdnet.com/article/backdoor-found-in-zte-android-phones/.

## Federal Policies

In recent years, the federal government has attempted to build a legal bulwark to keep untrustworthy foreign technology out of U.S. supply chains. This section examines four major policies and programs within this new regulatory regime. The first is Section 889 of the 2019 NDAA, which prohibits federal agencies from using equipment and services provided by five Chinese tech companies and working with contractors that used covered equipment. The second is Title 2 of the SECURE Technology Act, which created a federal council to analyze supply chain security threats and recommend the removal or exclusion of certain technologies. The third is the ICTS rule, which allows the Commerce Department to review and block purchases of certain equipment and services across the public and private sector.[24] The fourth is the Secure and Trusted Communications Networks Act, which prohibited FCC funds from being used to buy certain foreign ICTS. This section also briefly touches on other recent efforts by the FCC to block untrustworthy foreign technology from entering the U.S. market.

### *Section 889*

Section 889 of the 2019 NDAA is the first and most well-known regulation targeting foreign ICTS on the grounds of national security. Enacted in August 2018, the law bars federal agencies from procuring or otherwise using equipment and services provided by five named Chinese companies: Huawei, ZTE, Hikvision, Dahua, and Hytera. Section 889 also forbids federal agencies from working with contractors that use ICTS from those five firms and prohibits them from allocating grants or loans for the purchase of such equipment.*

While the statute's scope is relatively limited, its potential impact is enormous. The federal government purchases more than $100 billion worth of information technology from thousands of companies every year.[25] Disentangling even a single company from that expansive supply chain—not to mention five—is a considerable feat, especially when those companies dominate their respective niches of the tech sector.[26]

---

* The 2018 NDAA included a similar provision (Section 1634) prohibiting federal agencies from purchasing or otherwise using products or services provided by Kaspersky Lab, a Russian cybersecurity firm. For more information, see: National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017).

However, despite its ambitious goals, Section 889 contains some major flaws. One shortcoming is that the law does not apply retroactively. Agencies are thus allowed to continue using covered ICTS that they purchased before the law went into effect, which may undermine the security of their networks.[27] Another issue is the measure's rigidity. While policymakers authorized national security leaders to add new entities to the ban, they did not create any mechanism for taking entities off the list. This effectively means that barring an act of Congress, covered organizations are permanently excluded from the federal market, regardless of changes in the threat landscape.[28]

Perhaps more importantly, however, the federal government may lack the capacity to ensure contractors are following Section 889. Currently, contractors are responsible for self-certifying that their products and internal networks do not contain covered ICTS. [29] As with other federal acquisition regulations, contractors that violate Section 889 may face penalties, debarment, or prosecution. However, given the complexity of global supply chains and the scope of the measure, even contractors acting in good faith might unknowingly break the rule by including covered ICTS in their products or using it in their own systems. Additionally, inspecting the IT infrastructure—equipment, services, and components—of every contractor that does business with the federal government would require a staggering level of resources, making it difficult for agencies to conduct effective oversight.

Indeed, implementing Section 889 has already proven to be a challenge. Some contractors have, for instance, required extra time to sever ties with covered Chinese tech companies.[30] There have also been instances when covered ICTS has found its way onto federal networks. Multiple federal departments and agencies, including the U.S. Army, U.S. Air Force, and the Drug Enforcement Administration, have purchased technologies covered by Section 889 after the law went into effect.[31] In some cases, the purchases were reportedly made through the GSA Advantage portal, an ecommerce platform where agencies can buy products that have been vetted by the General Services Administration. These violations of Section 889 came to light through investigations by journalists and industry watchers, not public disclosures by the federal government.

Even without these flaws, Section 889 alone would not be an optimal framework for addressing foreign technology threats. Different federal agencies have different risk tolerances. Certain foreign ICTS might be deemed unsafe for all government use, but others might be considered dangerous for some use cases but safe for others. The one-size-fits-all approach of Section 889 cannot accommodate these nuances. The federal

government needs a more customizable and dynamic strategy to address foreign technology threats.

### *Title 2 of the SECURE Technology Act*

The SECURE Technology Act, passed in December 2018, laid the groundwork for a more nuanced and nimble approach.[32]

Title 2 of the law permitted federal agencies to withhold contracts from vendors that present supply chain security risks.[33] Agencies are required explain the reasoning behind their decisions and give the providers in question an opportunity to respond, removing any ambiguity about the threats a product poses and fending off potential legal challenges. Armed with this authority, agencies have the freedom to make procurement decisions based on their own levels of risk tolerance.

The law also established an interagency body to act as a clearinghouse for information on untrustworthy ICTS and coordinate efforts to eliminate them from government networks. This organization, called the Federal Acquisition Security Council (FASC), has two primary duties.[34] The first is to gather and share information related to supply chain security risks with federal agencies and other organizations across the public and private sectors.* This may include information from a variety of sources, including the risk assessments and other intelligence that agencies have used to justify procurement prohibitions.

The council's second responsibility is to evaluate the risks posed by particular technologies and recommend actions to address them. Those recommendations may come in the form of exclusion orders (bans on future procurements of specific ICTS or from specific manufacturers) or removal orders (directives to purge networks of specific existing ICTS). Like individual agencies, the FASC must explain the reasoning behind its recommendations and give the providers in question an opportunity to respond.[35] Those recommendations are then reviewed by the director of national intelligence and secretaries of defense and homeland security, who then decide whether to issue binding removal or exclusion orders to federal agencies.[36] These orders would build off the existing Section 889 regime and give the government more flexibility to target specific applications of foreign ICTS rather than relying on blanket bans.

---

* The ICT Supply Chain Risk Management Task Force, housed within the Cybersecurity and Infrastructure Security Agency (CISA), is responsible for running information sharing efforts on behalf of the FASC.

With its authorities finalized in August 2021 and policymakers still revising its procedures behind the scene, the FASC is just getting off the ground. In the years ahead, the council has the potential to play a central role in addressing foreign technology threats at the federal level. It can ensure that threats to intelligence are quickly shared across the government and broader national security community, and when necessary, push for government-wide action to eliminate untrustworthy ICTS. As we will discuss in a later section, it may also have a role to play in helping state and local governments restrict their use of untrustworthy foreign ICTS.

***The ICTS Rule***

Similar to the FASC, the ICTS rule gives the federal government—specifically the Commerce Department—the ability to restrict the purchase and use of ICTS provided by untrustworthy foreign entities. However, the authorities granted under the ICTS rule extend not just to federal agencies but to every entity under U.S. jurisdiction.

The rule, which traces its roots to an executive order signed in May 2019, grants the Commerce Department the authority to review ICTS transactions involving entities linked to "foreign adversar[ies]" and block any transaction that it deems as a national security threat.[37] The Biden administration is still working out the specifics of the measure, but an interim version published in January 2021 suggests the rule could have an expansive scope. As it stands, the department will have jurisdiction over all transactions between U.S. persons (individuals, businesses, governments, etc.) and foreign entities that involve six types of ICTS: critical infrastructure, networking systems, widely-used personal data hosting systems, widely-used digital applications, widely-used surveillance and monitoring systems, or emerging technology (e.g., artificial intelligence, quantum computing, autonomous systems).

Under the rule, the Commerce Department can block or unwind any transactions that involve a "foreign adversary" and "pose an undue or unacceptable risk" to national security. As of this writing, the measure explicitly names China, Cuba, Iran, North Korea, Russia, and Venezuela as foreign adversaries.

The ICTS rule represents a major expansion of the federal government's jurisdiction over the private sector. Federal agencies already have the ability to intervene in foreign business activities through sanctions, export controls, and investment screenings, but these authorities generally do not cover U.S. purchases of foreign products and

services.* Additionally, the scale and scope of these authorities are relatively limited. The Committee on Foreign Investment in the United States, which reviews foreign investments in U.S. companies for national security threats, processed an average of 152 cases each year between 2008 and 2020.[38] By contrast, under the ICTS rule, the Commerce Department would be expected to review potentially thousands—if not tens of thousands—of transactions each day.[39]

The sheer magnitude of the ICTS rule creates challenges for both the department that enforces it and the businesses that fall under its purview. Performing oversight at this scale will require substantial resources. The Bureau of Industry and Security, the agency within the Commerce Department responsible for enforcing the ICTS rule, currently has 16 positions and about $4.7 million devoted to the program.[40] BIS asked lawmakers for an additional 114 positions and $36.2 million in its 2023 budget request, but it is still unclear whether the department will get sufficient support from Congress.

For the private sector, the rule also introduces new uncertainties into the messy process of ICTS procurement. Keeping pace with rapid technological change is already a challenge for businesses, and under the rule, they risk having IT projects stalled or blocked altogether by federal regulators. The Commerce Department is currently exploring a licensing framework that would let businesses have transactions pre-approved, but the details of that process have not yet been finalized. Later in this brief, we discuss how implementing a sanctions-based framework, rather than relying on licenses, would maximize the rule's effectiveness and minimize the costs of compliance.

### *FCC Measures*

The FCC also has a handful of policy levers at its disposal to keep untrustworthy foreign ICTS out of U.S. networks.

---

* Though it is not their primary goal, many of the sanctions administered by the U.S. Department of the Treasury effectively function as procurement prohibitions. When a person or organization is classified as a "specially designated national" (SDN), all U.S. persons—individuals, companies, governments—are forbidden from conducting business with them, which includes purchasing their products. The SDN list currently includes 155 Chinese entities, but none of the Section 889 firms.

Under the 2020 Secure and Trusted Communications Networks Act, the FCC is required to maintain a list of vendors that "pose an unacceptable risk to the national security of the United States, and recipients of FCC funds are forbidden from purchasing ICTS provided by those firms."[41] As of this writing, the commission's "covered list" includes nine Chinese firms—the five Section 889 companies, China Mobile International USA, China Telecom Americas Corp., Pacific Networks Corp, and China Unicom (Americas) Operations Ltd.—as well as the Russian cybersecurity firm Kaspersky Lab.[42] Hundreds of public and private entities receive subsidies from the commission each year. Barring those organizations from purchasing compromised ICTS could go a long way to securing the country's communications infrastructure.

The law also required the FCC to create a program to assist small service providers in replacing covered ICTS that already reside in their networks.[43] In 2020, Congress allocated about $1.9 billion to the Secure and Trusted Communications Networks Reimbursement Program, which would initially focus on "ripping and replacing" equipment from Huawei and ZTE. However, the effort has proven to be far more expensive, with the first wave of applicants asking for more than $5.6 billion in reimbursements.[44] It remains unclear whether the program will receive additional funds from Congress or be expanded to cover replacements of ICTS from other covered companies.[45] As we will discuss in a later section, increasing federal support for similar rip and replace programs will be crucial for eliminating potentially untrustworthy technologies from government supply chains.

FCC commissioners are also currently considering using the agency's equipment authorization process to curtail the use of certain foreign technologies.[46] Under current laws, almost all products capable of emitting a radio signal—cell phones, Bluetooth devices, telecommunications equipment, etc.—must receive FCC authorization before they can be sold in the United States. In June 2021, the commission requested public comments on a proposal to prohibit future authorizations of ICTS produced by companies on the FCC covered list.[47] The fate of the rule remains to be seen—as of this writing, commissioners have yet to put the measure to a vote. Should it be approved, the commission would effectively make it illegal to import, sell, and use most (if not all) new products manufactured by Huawei, ZTE, Hikvision, and the seven other covered companies within U.S. borders.

***Summary of Federal Policies***

Over the last five years, federal policymakers have steadily laid the groundwork for an effective defense against foreign technology threats. The SECURE Technology Act

created an ecosystem for sharing information on untrustworthy ICTS, empowered agencies to issue tailored procurement prohibitions, and established a process for scaling those prohibitions across the government when necessary. The ICTS rule enabled federal policymakers to lead nationwide crack downs on foreign technology threats. The FCC's covered list added an additional level of security to the U.S. telecommunications grid, and the commission's rip and replace program helps organizations plug the existing vulnerabilities in their networks. Despite its flaws, Section 889 set a precedent for pursuing government-wide procurement prohibitions.

The landscape of federal procurement prohibitions is complex, with policies and programs overlapping and intersecting. However, each serves a distinct purpose, enabling national security leaders to tailor procurement prohibitions to meet the needs of different types of organizations. To be sure, these authorities are still relatively new, and it is critical that each measure is properly scoped and implemented. Policymakers have the authority to crack down on foreign technology threats, and now they must wield that power effectively. We offer recommendations for strengthening federal supply chain security efforts later in the report.

## State Policies

The federal government cannot unilaterally purge U.S. networks of compromised foreign technology. A wide variety of public services and critical infrastructure systems are managed by state and local governments, so efforts to defend against foreign technology threats must also have their buy-in.

However, state and local governments have generally not revised their procurement policies to address the issue of foreign technology threats. In recent years, nearly 1,700 public entities have purchased ICTS covered under Section 889, introducing potential vulnerabilities into the networks of public schools, universities, hospitals, prisons, public transit systems, and government offices nationwide. Just five states—Florida, Georgia, Louisiana, Texas, and Vermont—have adopted measures to restrict the purchase of untrustworthy ICTS on national security grounds, and these regulations are generally not structured to deal with foreign technology threats effectively. We outline the strengths and weaknesses of each later in this section.

State and local governments must take foreign technology threats seriously even if they do not face the same risks as federal agencies like DOD. Foreign hackers have already shown an interest in targeting non-federal entities. At least six state governments had their networks breached by a state-sponsored Chinese hacking group between May 2021 and February 2022, and countless local government entities fell victim to Chinese hackers during the Microsoft Exchange Server data breach in early 2021.[48] Should the Chinese government or other competitors exploit foreign ICTS in a similar fashion, thousands of state and local governments may find themselves exposed to potentially devastating breaches. Even if governments are not targeted directly, the ICTS they deploy might be used to compromise nearby critical infrastructure—a recent FBI investigation revealed that Huawei equipment deployed near military bases could be used to capture or disrupt communications regarding the U.S. nuclear arsenal.[49]

Given these risks, removing untrustworthy foreign ICTS from state and local networks is a national security imperative. In recent years, however, many agencies have continued introducing untrustworthy technologies into their networks. In this section, we explore the extent to which state and local governments are buying ICTS prohibited at the federal level under Section 889 and discuss the strengths and

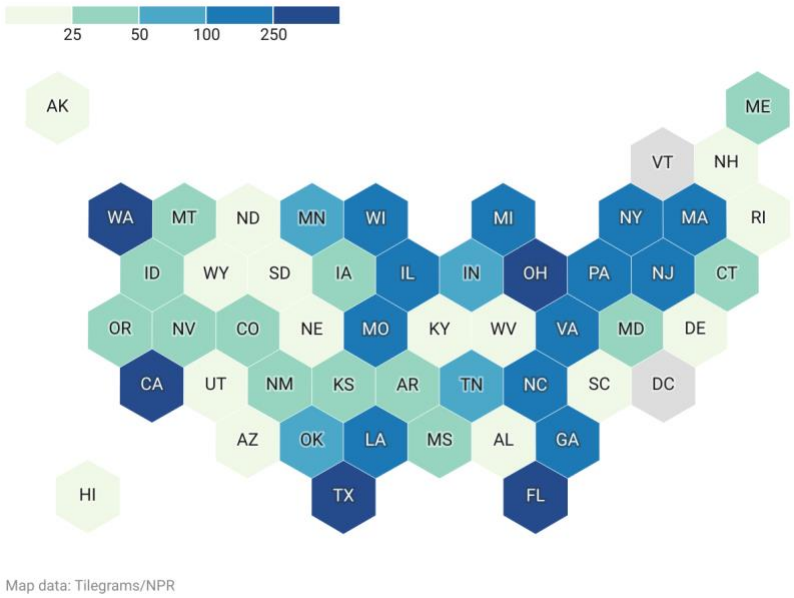
weaknesses of existing state-level regulations on foreign ICTS procurement.* We conclude with a discussion of the roles federal, state, and local policymakers should play in developing a cohesive approach to ICTS supply chain risks.

### *Who's Buying What?*

Between 2015 and 2021, at least 1,681 state and local governments purchased equipment and services tied to the five companies named in Section 889. Every state except Vermont had at least one state or local government entity procure ICTS covered under Section 889 (there were also no purchases in Washington, D.C.). Collectively, these entities conducted nearly 5,700 transactions involving a wide range of covered equipment including but not limited to smartphones, surveillance cameras, temperature scanners, handheld radios, and networking equipment.[50] Figures 1 and 2 show the total number and value of government transactions that involved equipment from Huawei, ZTE, Hikvision, Dahua, and Hytera in each state. Our analysis relies on data provided by GovSpend, a company that tracks federal, state, and local government procurement.

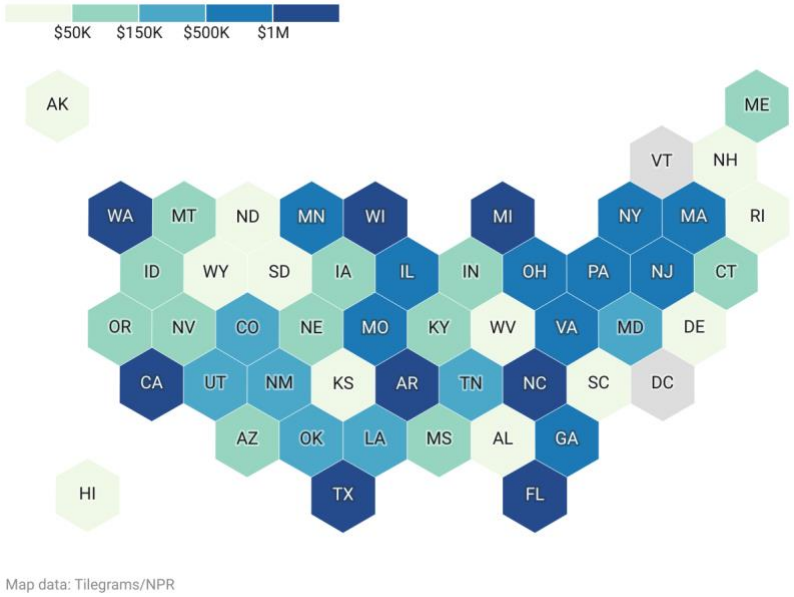
* We do not attempt to analyze the landscape of procurement prohibitions at the local level due to the sheer number of local government entities that exist across the United States. A cursory review found a single locality—the city of Suffolk, Virginia—that has restricted the purchase of Chinese technology on the grounds of national security. For more, see: City of Suffolk, *Addendum #1: Exterior Dome PTZ Cameras* (Suffolk, VA; Purchasing Division, 2018), http://apps.suffolkva.us/bids/files/2217_Addendum_1_-_PTZ_Cameras.pdf.

Figure 1. Number of State and Local Government Transactions Involving Covered ICTS by State, 2015-2021 (Including D.C.)




Source: CSET analysis of GovSpend data (see Appendix A for more details).

Figure 2. Value of State and Local Government Transactions Involving Covered ICTS by State, 2015-2021 (Including D.C.)




Source: CSET analysis of GovSpend data.

The total value of these purchases was approximately $45.2 million. While the scale of transactions may seem small in terms of monetary value, it is significant in terms of potential risk. Each piece of covered equipment represents a potential entry point into users' networks, regardless of its cost. The fact that untrustworthy technology was integrated into the networks of nearly 1,700 state and local government entities is far more relevant to national security than the total transaction value. If exploited properly, even small, inexpensive components can undermine the security of the broader government systems they connect to, allowing hackers to leapfrog from one system to another.

Our findings should be interpreted as a partial glimpse into state and local government purchasing behavior rather than a comprehensive review. Procurement records were scraped from unstandardized public documents, which can sometimes omit or misrepresent details on equipment or services. Furthermore, GovSpend does not collect data on every state and local government entity in the United States, meaning some purchases may be excluded from our analysis (see Appendix B for more information on our methodology).

Procurement patterns among individual government entities were highly stratified. About 87 percent (1,463) of the public entities in our dataset conducted five or fewer transactions involving covered ICTS, and about half (858) had a single recorded purchase. On the other end of the spectrum, there were 37 organizations that conducted 20 or more transactions involving covered ICTS, and nine that made 50 or more purchases. These nine buyers—all but one of which are involved in public education—accounted for more than one-third of all recorded transactions.

While a wide variety of public entities have purchased covered ICTS, including transit authorities, utilities departments, judicial systems, and state and local government agencies, the technologies appear to be especially popular within public education systems. Public school districts, colleges, and universities collectively conducted 4,283 transactions for covered ICTS, about three-quarters of all the purchases recorded in our dataset (see Table 1). Of the 56 organizations that spent more than $100,000 on untrustworthy Chinese technology, 50 were involved in public education.

Table 1. Number of State and Local Governments Buying Covered ICTS by Organization Type, 2015-2021 (Including D.C.)

| Organization Type | Entities | Total Transactions | Total Spending |
|---|---|---|---|
| **Public School** | 938 | 3,693 | $20,346,606 |
| **Local Government** | 482 | 1,171 | $6,448,427 |
| **State University/College** | 161 | 590 | $17,205,618 |
| **State Government** | 49 | 124 | $591,138 |
| **Public Utility** | 23 | 52 | $372,191 |
| **Public Hospital** | 10 | 19 | $43,810 |
| **Public Transit** | 10 | 15 | $89,050 |
| **Judiciary** | 8 | 16 | $57,277 |
| **Total** | **1,681** | **5,680** | **$45,154,118** |

Source: CSET analysis of GovSpend data.

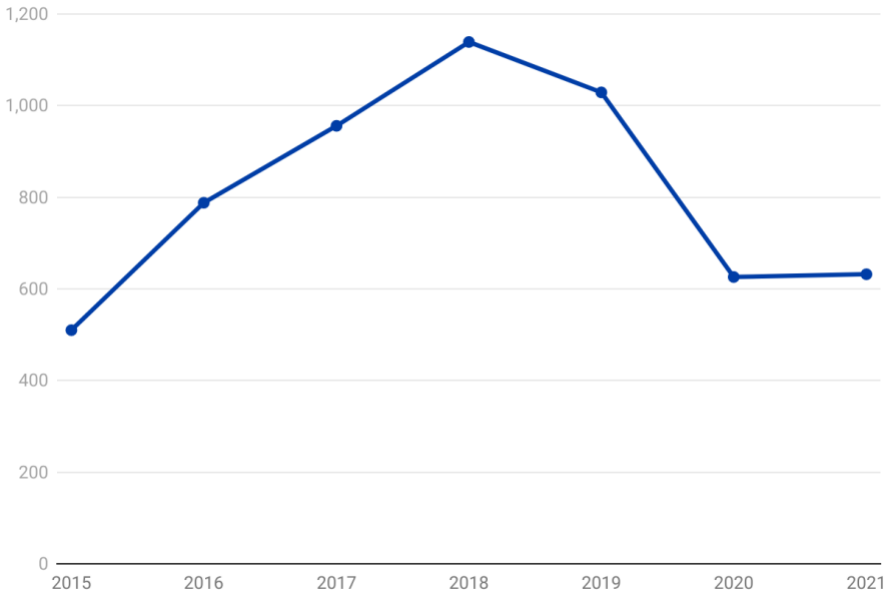
There are a few reasons why public schools, colleges, and universities comprise such a large share of the transactions in our dataset. First and foremost, they make up an outsized portion of the overall market. Universities and school districts typically operate more facilities than other public entities, and each school and campus building requires its own networking infrastructure and surveillance system.

Additionally, procurement officials at educational institutions may have less security expertise than those at other government agencies, and are thus more likely to award contracts based primarily on cost. Such decisions will favor Chinese ICTS due to its relative affordability.[51] This lack of internal security expertise may also lead public schools to be less discrete when disclosing procurement information. Revealing details about the equipment on a network clues bad actors in on the system's vulnerabilities and compromises its security. As such, government agencies with more security expertise may withhold more information on their ICTS purchases when filling out public documents, which would make them less likely to appear in the GovSpend dataset.

Most of the recorded transactions involved small batches of smartphones, radios, cameras, and other one-off items. Among the most popular products were Hikvision dome and bullet cameras, Hikvision network video recorders, Dahua fisheye cameras, Hytera portable two-way radios (particularly the PD502 model), and Huawei routers and networking equipment. Also among the most popular products were ZTE's mobile Wi-Fi hotspots, Speed smartphones, and SPro smart projectors. However, many of the highest spending organizations appear to have invested in more systematic, enterprise-wide deployments of covered ICTS. The single largest buyer in our dataset, a mid-size public university in Michigan, invested some $15.1 million in Huawei LTE networking equipment (nodes, transceivers, base stations, and power systems) and related support services between 2015 and 2021. Similarly, a pair of public school districts in northeast Arkansas each spent more than $1 million on Hikvision surveillance systems, and a charter school district in a major Texas city spent more than $550,000 on Hytera two-way radios.

Procurement records show state and local governments continued buying covered Chinese ICTS after the federal government raised concerns about the security of the equipment. However, the number of transactions has fallen since the passage of Section 889 in August 2018, as shown in Figure 3. In the vast majority of these transactions, public entities did not award contracts directly to the Chinese manufacturers, but rather to third-party distributors of their technology. These "middle-man" vendors can mask the origin of their products, which creates major challenges for organizations aiming to keep certain equipment and services off their networks. As we will discuss in the following section, these third-party transactions would still be considered legal under many of the existing state-level regulations on Chinese ICTS, which prohibit transactions with specific vendors rather than procurement of specific technologies.

Figure 3. Annual State and Local Government Transactions Involving Covered ICTS, 2015-2021 (Including D.C.)




Source: CSET analysis of GovSpend data.

### *State Procurement Prohibitions*

Few states have amended their procurement policies to weed out untrustworthy foreign ICTS from their supply chains. Our review of state-level regulations found that only five states—Florida, Georgia, Louisiana, Texas, and Vermont—had enacted measures to limit the procurement of foreign ICTS on the grounds of national security (see Table 2).[52]

Each of the five states that have passed procurement prohibitions took a slightly different approach, some of which are more effective than others. Some measures forbid states from doing business directly with foreign vendors while others focus on the specific technologies they produce. The scope of the prohibitions also vary widely: for instance, the Louisiana measure targets only the five Chinese companies included in Section 889 while Texas bars all Chinese, Russian, North Korean, and Iranian companies from being awarded certain state contracts.

In this section, we provide a brief overview of the strengths and weaknesses of each state's approach to addressing foreign technology threats, and in the following section, we offer recommendations for building a more cohesive, nationwide approach to removing untrustworthy foreign ICTS from U.S. supply chains.

Table 2. Foreign ICTS Procurement Prohibitions by State (Including D.C.)

| State | Action Taken |
|---|---|
| Alabama | n/a |
| Alaska | n/a |
| Arizona | n/a |
| Arkansas | n/a |
| California | n/a |
| Colorado | n/a |
| Connecticut | n/a |
| Delaware | n/a |
| District of Columbia | n/a |
| Florida | Exec. Action (2022) |
| Georgia | Law (2022) |
| Hawaii | n/a |
| Idaho | n/a |
| Illinois | n/a |
| Indiana | n/a |
| Iowa | n/a |
| Kansas | n/a |
| Kentucky | n/a |
| Louisiana | Laws (2020-21) |
| Maine | n/a |
| Maryland | n/a |
| Massachusetts | n/a |
| Michigan | n/a |
| Minnesota | n/a |
| Mississippi | n/a |
| Missouri | n/a |
| Montana | n/a |
| Nebraska | n/a |
| Nevada | n/a |
| New Hampshire | n/a |
| New Jersey | n/a |
| New Mexico | n/a |
| New York | n/a |
| North Carolina | n/a |
| North Dakota | n/a |
| Ohio | n/a |
| Oklahoma | n/a |
| Oregon | n/a |
| Pennsylvania | n/a |
| Rhode Island | n/a |
| South Carolina | n/a |
| South Dakota | n/a |
| Tennessee | n/a |
| Texas | Law (2021) |
| Utah | n/a |
| Vermont | Exec. Action (2019) |
| Virginia | n/a |
| Washington | n/a |
| West Virginia | n/a |
| Wisconsin | n/a |
| Wyoming | n/a |

Source: CSET analysis of GovSpend data.

### Louisiana

The state that has most closely mirrored the federal government's approach to covered ICTS is Louisiana. In 2020 and 2021, Louisiana policymakers passed a pair of laws that banned all state government agencies and publicly funded schools, universities, and other educational institutions from buying ICTS covered under Section 889.[53]

There are both benefits and drawbacks to Louisiana's approach to foreign technology threats. By aligning its procurement practices to federal regulations, the Louisiana government can automatically heed the guidance of national security leaders without going through the process of amending rules every time a problematic vendor is identified. However, tying the fate of the state to the federal policymaking process is only beneficial if that process is effective. If Section 889 proves to be too limited in scope, or if policymakers are too slow to update the list as new threats emerge, then Louisiana may find itself vulnerable.

### Texas

Texas took a different approach to addressing foreign technology threats, focusing specifically on critical infrastructure and expanding the scope of covered countries. In June 2021, the state enacted the Lone Star Infrastructure Protection Act (SB-2116), which restricted state agencies from awarding "critical infrastructure" contracts to companies linked to China, Russia, Iran, or North Korea.* Furthermore, the measure forbade private companies from entering into agreements with these companies if the partnership would grant them remote or direct access to critical infrastructure.

Though this expanded scope may appear to make SB-2116 more effective, the law also contains a major loophole. By focusing specifically on companies—and not the equipment and services they produce—the law leaves the door open for compromised ICTS to enter government networks through third-party distributors. Purchasing a Hikvision surveillance camera directly from Hikvision would be illegal, but purchasing the exact same camera from a local vendor would not. If the goal of a procurement ban

* Specifically, the company cannot be headquartered in, or controlled by the government or citizens of, any of the listed countries. Additionally, the law classifies communications infrastructure systems, cybersecurity systems, electric grids, hazardous waste treatment systems, and water treatment facilities as critical infrastructure: Lone Star Protection Act, Texas S.B. 2116, 87th Legislature (2021).

is to keep compromised equipment and services out of government networks, it must target the product, not the seller.

### Georgia

Georgia's Senate Bill 346, signed into law in May 2022, prohibits any company "owned or operated" by the Chinese government from applying for state contracts.[54] Companies are required to certify they are not owned by the CCP when submitting contract proposals, and those that lie about their affiliation face a $250,000 minimum fine.

Like its Texas counterpart, SB-346 focuses on ICTS vendors rather than explicitly targeting the equipment and services they produce, which creates a loophole through which third-party vendors can legally sell compromised ICTS to the state government. Furthermore, the measure does not specify which companies are subject to the ban, which may make it difficult to enforce. Some may interpret the law as applying only to Chinese state-owned enterprises while others might argue that a much longer list of Chinese companies are "owned or operated" by the state.[55]

In July 2022, the American Legislative Exchange Council, a conservative nonprofit that facilitates collaboration between state legislators and private sector representatives, published a "model policy" based on the Georgia law.* This draft legislation contains the same loopholes as SB-346, and state laws modeled on this text will be ineffective.

### Vermont

In Vermont, government leaders opted for executive action over legislation to address foreign technology threats. In February 2019, Vermont's chief information officer

---

* "An Act to Prohibit State Contracts With Chinese Government-Owned or Affiliated Technology Manufacturers," *American Legislative Exchange Council*, accessed October 2022, https://alec.org/model-policy/an-act-to-prohibit-state-contracts-with-chinese-government-owned-or-affiliated-technology-manufacturers/. ALEC describes itself as dedicated to the principles of limited government, free markets, and federalism. Between 2010 and 2018, more than six hundred state and federal laws were passed based on the organization's model policies. For more, see: "About ALEC," *American Legislative Exchange Council*, accessed September 2022, https://alec.org/about/; Yvonne Wingett Sanchez and Rob O'Dell, "What is ALEC? 'The most effective organization' for conservatives, says Newt Gingrich," *USA TODAY*, April 3, 2019, https://www.usatoday.com/story/news/investigations/2019/04/03/alec-american-legislative-exchange-council-model-bills-republican-conservative-devos-gingrich/3162357002/.

issued a directive prohibiting state agencies from purchasing equipment and services produced by the five companies listed in Section 889 as well as the Russian cybersecurity firm Kaspersky Lab.[56] Like Section 889, the measure forbids the state from working with vendors that use those systems. However, unlike Section 889, it also required agencies to review their IT infrastructure for covered ICTS and begin phasing out those products within 90 days.

Vermont's approach to foreign technology threats is relatively effective. The directive addresses both past and future procurements of covered ICTS, and targets specific technologies rather than companies that manufacture them.

Still, the strategy is not without shortcomings. While enacting procurement bans through executive action is faster than through legislation, this approach also means the regulations are easier for future governors to overturn. Furthermore, the state's directive did not set aside funds to rip and replace covered ICTS within government networks. One of the major appeals of Chinese ICTS is its low cost. Agencies will likely need additional funding in order to replace this equipment with more expensive alternatives. The directive also lists the specific companies covered by the ban instead of referencing any particular federal regulation, meaning the measure will not automatically update as the threat landscape changes.

### Florida

Florida's Executive Order 22-216, signed by Governor Ron DeSantis in September 2022, is the broadest of the five state-level procurement prohibitions. The order seeks to bar state agencies from buying or using any ICTS that is prohibited or restricted at the federal level, and also from buying or using ICTS that poses "an undue or unacceptable risk to the safety and security of Florida."[57] Furthermore, the order aims to prevent state agencies from purchasing or using ICTS provided by entities "owned, controlled by, or domiciled in a foreign country of concern as much as feasibly possible." Currently, seven countries are included in that list: China, Russia, Iran, North Korea, Cuba, Venezuela, and Syria.[58]

Like its counterparts in Louisiana and Vermont, the Florida prohibition focuses on specific ICTS and not specific vendors, avoiding the loophole that would allow agencies to buy untrustworthy technology from third-party vendors. It is also directly linked to federal prohibitions, meaning the procurement policies will automatically update as the threat landscape changes. Requiring states to limit their use of ICTS sourced from countries of concern "as much as feasibly possible" is also preferable to

blanket bans. Cutting out all ICTS from China, for example, would be prohibitively expensive, if not impossible.

The order also grants the state's Department of Management Services the authority to identify and ban untrustworthy ICTS based on "relevant materials . . . from any government agency, cybersecurity firm, or expert." It is critical for state agencies to consider all available information when making procurement decisions, but this broad definition of acceptable documentation may be mistakenly interpreted to mean that evidence from a single firm or expert could be used to justify a prohibition. Procurement prohibitions must be based on a thorough review of evidence from multiple sources to ensure that only legitimately unsafe ICTS gets banned. As they implement the executive order, Florida officials should make sure they create a robust review process that ensures the department uses its new authorities effectively and judiciously.

***Summary of State Policies***

Overall, state-level approaches to foreign technology threats have left much to be desired. Few states have enacted measures aimed at removing untrustworthy foreign ICTS from government supply chains, and the effectiveness of those regulations varies widely.

Given the complexity of the global ICTS supply chain, procurement prohibitions will only be effective if they target specific technologies from specific manufacturers rather than specific sellers. Three states—Florida, Louisiana, and Vermont—have taken this approach. Measures that target vendors, such as those in Georgia and Texas, may create a false sense of security without addressing the risks posed by foreign ICTS. As shown in the GovSpend data, the vast majority of covered ICTS is purchased through third-party distributors rather than with the manufacturers themselves. These transactions would be considered legal under the Georgia and Texas laws. Georgia's SB-346 is also unclear about the companies that fall under its scope, making it difficult to enforce and increasing the likelihood of litigation. The fact that Georgia's law is being held up as a model for other states to follow raises serious concerns about future state-level efforts.

While they correctly target technologies rather than vendors, the measures enacted in Louisiana and Vermont are not scoped in a way to effectively deal with foreign technology threats. These policies, which are rooted in Section 889, are likely too

narrow and would need to be updated regularly to accommodate changes in the threat landscape.

In general, we find that state and local governments would benefit from aligning their procurement practices with those of the federal government rather than creating their own definitions of untrustworthy ICTS. Federal policymakers have already constructed a robust process for determining whether certain products and services pose national security threats, and it would behoove state and local agencies to piggyback off this federal guidance. In the following section, we discuss how these policymakers can build federal prohibitions into their own procurement processes.

## Policy Recommendations

While every level of government must play a role in addressing foreign technology threats, federal policymakers should be responsible for spearheading these efforts. With its resources and intelligence capabilities, the U.S. government is in the best position to identify vulnerable ICTS and develop strategies to eliminate them from nationwide supply chains, and recent measures give it the proper authorities to do so. Under Title 2 of the SECURE Technology Act, federal agencies can purge untrustworthy technology from their supply chains and policymakers can scale those prohibitions across the government as they see fit. The ICTS rule—if implemented properly—allows the Commerce Department to extend prohibitions to the broader U.S. market as well.

However, defending the United States against the threats posed by foreign technology will require state and local officials to align their procurement decisions with federal guidance. This means complying with the Commerce Department's mandatory orders and proactively piggybacking off of federal procurement prohibitions when necessary.

In this section, we offer recommendations on how the federal government can strengthen its approach to procurement prohibitions and enable government entities to address the risks associated with foreign ICTS. We also discuss how state and local government officials can align their procurement policies with federal guidance to create a more cohesive, nationwide strategy for addressing foreign technology threats.

### *Effectively Implement the ICTS Rule*

The ICTS rule has the potential to significantly strengthen the federal government's ability to crackdown on foreign technology threats across the broader U.S. market, but only if the Commerce Department implements the authority effectively. This requires leaders to allocate enough funding and staff to implement the rule, create the proper information sharing channels, and develop a regulatory approach that maximizes the measure's impact while minimizing its economic and organizational costs.

The Commerce Department's recent budget requests indicate that the BIS is charged with implementing the ICTS rule.[59] The agency, which today primarily manages and enforces the government's export control regime, seems like a natural fit for this new authority. Under its current remit, BIS staffers have gained a deep understanding of the national security implications of technology and experience working with industry, both of which will be critical for implementing the ICTS rule.

The department's 2023 budget submission requested an additional 114 positions and $36.2 million to support BIS implementation of the ICTS rule. As it stands, the agency has 16 positions and about $4.7 million devoted to the program.[60] It remains to be seen whether Congress will meet the agency's request and whether that level of funding will prove sufficient for enforcing the ICTS rule. BIS is already widely considered to be under-resourced, and given the broad scope of its new authorities, it will likely require a significant increase in both staffing and funding. Implementing the ICTS rule effectively will also require BIS to increase coordination and information sharing with other federal agencies, like the DOD, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Telecommunications and Information Administration.

The agency's funding and staffing needs will depend on how exactly the ICTS rule is implemented. Commerce has committed to using a voluntary licensing framework that allows businesses to have their purchases of foreign ICTS preapproved by the department.[61] This system would allow businesses to buy new technologies without having to worry that regulators will block or roll back the transaction, but it would also force the department to review a potentially enormous number of transactions.[62] According to internal estimates, up to 4.5 million U.S. entities import foreign technologies covered by the rule—if each of those entities applied for just one license every year, the department would be responsible for processing upwards of 87,000 licenses per week.[63] The rule is unlikely to be effective if regulators are constantly drowning under a flood of applications.

Some experts have argued that a more productive approach would be to adopt a sanctions-based framework to foreign ICTS imports instead of relying on voluntary licensing.[64] Under such a framework, regulators would work with the national security community to determine which entities qualify as "foreign adversaries" and which of their products and services present potential security risks. Once those products are added to the department's covered list, all U.S. persons would be prohibited from purchasing them. This framework, which echoes Section 889 and existing sanctions frameworks, would be far less taxing for both the department and industry than obtaining approvals on a case-by-case basis. We find this approach to be the most effective path forward.

### *Block FCC Equipment Authorizations for Covered Entities*

Through its equipment authorization process, the FCC can directly control what ICTS can be legally sold in the United States. Commissioners should use this authority to keep untrustworthy foreign technologies from entering the U.S. market.

Under a 2021 law, commissioners are required to vote on whether to prohibit new authorizations of equipment manufactured by entities on the FCC covered list.[65] By approving this order, the commission can effectively stop all U.S. entities—both public and private—from buying most of the technology manufactured by Huawei, ZTE, Hikvision, and seven other foreign companies deemed to pose national security risks. The measure may not apply retroactively, meaning ICTS that is already authorized would still be legal to sell.[66] Still, banning new authorizations would mark an inflection point in the fight against foreign technology threats. Existing deployments of covered ICTS will eventually need to be phased out, and the order would ensure they are replaced with more trustworthy alternatives. Such a measure would create a baseline level of security upon which future procurement prohibitions from the FASC, Commerce Department, and other organizations.

### *Align State and Local Procurement Policies with Federal Guidance*

State and local policymakers should not be expected to independently analyze and address the threats posed by foreign technology, but it would behoove them to align their own procurement practices with the rules set by the federal government.

This will not necessarily require new regulations. State and local governments are already subject to the orders issued under the Commerce Department's ICTS authority. Complying with the rules will automatically improve the security of state and local networks.

However, if the Commerce Department does not implement the ICTS rule effectively, state and local governments may benefit from taking additional policy actions. The Commerce Department may not prohibit all of the ICTS banned at the federal level (based on FASC recommendations, for example), or it may fail to effectively implement the rule altogether. In these cases, state and local governments would still be legally allowed to buy untrustworthy foreign ICTS.

Should the ICTS framework fail to fully address foreign technology threats, state and local policymakers should enact policies to prevent their governments from buying ICTS covered by federal procurement bans. Doing so would allow state and local

governments to stay up to date on the latest threat intelligence without expending any of their already limited resources on the necessary research and intelligence. Piggybacking off of federal guidance would ensure regulations are scoped properly and focused on the appropriate threats.[67]

Section 1(B) of Florida's Executive Order 22-216, which bars state agencies from using ICTS "any federal agency has prohibited . . . because of national security concerns," could serve as a model for other jurisdictions. However, state and local policymakers should avoid creating their own definitions of "covered ICTS." As discussed in the previous section, these definitions often miss the mark, casting too wide of a net or targeting the wrong vendors or products. Furthermore, the costs of maintaining and complying with 50-plus different standards would be exorbitant for both government agencies and their contractors, while the potential benefits are minimal at best.

To be sure, federal procurement prohibitions may themselves be mistargeted or out of date in some cases. But unifying every level of government around a defined set of untrustworthy technologies will likely be more effective than creating a patchwork of procurement prohibitions across jurisdictions.

***Create and Share a Master List of Untrustworthy Foreign ICTS***

Beyond subsidizing rip and replace efforts, federal policymakers can make it easier for state and local governments—as well as other public and private organizations—to secure their networks by publishing a list of untrustworthy foreign ICTS.

Today, there is no single, publicly available "master list" when it comes to untrustworthy foreign ICTS. Section 889 and the FCC's covered list both explicitly name companies that pose security risks, but each includes different entities. To date, neither the FASC nor Commerce Department has issued a list of prohibited vendors. This lack of consistent, up-to-date information makes it difficult for public- and private-sector procurement officers to ensure they steer clear of untrustworthy foreign ICTS.

This "master" covered list might include information on specific equipment and services, the companies that produce them, and, when appropriate, the risks they pose. It should also disclose that entities can and cannot buy the designated ICTS and what

federal authority each prohibition was issued under (e.g. the SECURE Technology Act).*

Using this list, state and local procurement officers would easily identify the ICTS they are explicitly barred from using (under Commerce orders) plus other foreign technologies that federal policymakers have determined to pose national security risks. Measures that link state and local procurement practices to federal prohibitions—in the vein of the Florida executive order—could refer explicitly to this list.

Federal policymakers must also help state and local governments put this list to use. Agencies like CISA already work closely with state and local governments on cybersecurity and supply chain security issues.[68] They should continue building those relationships and information sharing networks, using them to help agencies interpret federal directives and understand their exposure to untrustworthy ICTS. By bringing state and local entities into the fold, federal policymakers can lay the foundation for a more harmonized, nationwide approach to addressing foreign technology threats.

Not every state and local agency will have the bandwidth or expertise to utilize this information, so it is also critical that federal agencies work with them to determine what intelligence and information sharing channels are most useful. It would not be possible to perfectly target outreach to every state and local entity, but understanding the challenges that different agencies face when addressing foreign technology threats will ultimately strengthen the information sharing ecosystem.

***Support Rip and Replace Programs***

Federal policymakers can also enable state and local governments to address foreign technology threats by increasing support for rip and replace efforts like those pioneered at the FCC. Replacing compromised ICTS with more trustworthy alternatives can be a costly process in terms of both money and personnel. Public entities generally operate on tight budgets, and it is unlikely that they will muster the funds and political will to replace functional ICTS with more costly equipment. Furthermore, few public entities have the in-house expertise to lead a successful rip and replace effort.[69] The cybersecurity offices within these organizations are typically underfunded and understaffed (if they exist at all), and those that do have resources on hand will presumably prioritize more immediate security matters, such as combating

* The Treasury Department's "Sanctions List Search" application could serve as a model for this public-facing list. See: "Sanctions Search List," *Office of Foreign Assets Control*, accessed October 2022, https://sanctionssearch.ofac.treas.gov/.

ransomware, over the more abstract risks posed by foreign ICTS. [70] As such, we should not expect state and local governments to proactively rip and replace covered ICTS without federal support.

While federal agencies have offered some support to offset these costs, the funds are meager compared to the scope of the problem. For instance, the FCC's Secure and Trusted Communications Networks Reimbursement Program (SCRP), which provides funds to rip and replace equipment from Huawei and ZTE, was initially allocated some $1.9 billion. In the first round of applications, the commission received $5.6 billion in requests.[71] It is worth noting that to date, the SCRP does not cover replacements of ICTS from Hikvision, Dahua, Hytera, or the other companies included on the commission's covered list.[72] Should this equipment be included in the program, the reimbursement requests will be much higher. By increasing funding and expanding the scope of programs like the SCRP, the federal government can assist state and local policymakers to bolster their networks against Chinese technology threats.

If this funding cannot be made available immediately, federal policymakers should also support broader efforts to identify untrustworthy ICTS in existing government networks and supply chains. Today, many organizations, particularly state and local governments, do not fully understand their exposure to foreign technology threats. While mapping out potential points of failure does not fully mitigate their risks, such exercises will increase visibility into where problems might arise and help organizations more effectively triage their vulnerabilities.

To be sure, rip and replace programs are not a magic bullet for securing government networks. Every piece of equipment contains vulnerabilities, and the products and services that replace covered foreign ICTS may contain their own bugs and backdoors. Policymakers must therefore think critically about the costs and benefits of rip and replace programs before funding them. Different types of ICTS present different risks, and certain settings (e.g., power stations) require more security than others (e.g., university quads). Replacing every piece of untrustworthy tech currently installed on U.S. networks is not feasible, so resources must be allocated to the areas where they will have the greatest impact.[73] Rip and replace programs also divert resources away from other government services—such as education and infrastructure—and policymakers should consider the trade-offs of these reallocations.

## Conclusion

Defending against foreign technology threats requires coordinated action from policymakers at every level of government, with the federal government leading the way. With its resources and intelligence capabilities, the U.S. government is in the best position to identify vulnerable ICTS and develop strategies to eliminate them from nationwide supply chains, and recent measures give it the proper authorities to do so. State and local governments should align their own procurement practices with those federal guidelines. If a particular foreign technology is deemed too risky for federal agencies, state and local entities probably should avoid purchasing it as well.

Today, the U.S. approach to foreign technology threats falls far short of that ideal. Federal policies to keep untrustworthy ICTS out of government networks are not enforced effectively, and leaders are not fully utilizing their authority to monitor and mitigate supply chain threats. Only a handful of state governments have attempted to regulate the procurement of foreign technologies, and many of the measures that have been enacted fail to address the risks at hand. Local governments have been slow to act on foreign technology threats as well. All the while, state and local agencies have continued integrating untrustworthy technologies into schools, hospitals, prisons, public transit systems, and government offices around the country.

Federal policymakers must lead the effort to build a unified defense against foreign technology threats. Under the SECURE Technology Act, government leaders can tailor federal procurement prohibitions for different environments and applications. By providing the Commerce Department with the funds and staff to implement the ICTS rule—through a sanctions-based model—they can ensure untrustworthy technology stays out of public and private networks. Using these two authorities, policymakers can maintain effective procurement prohibitions that are current with the changing threat landscape. The FCC can also keep untrustworthy foreign ICTS from entering U.S. markets by blocking equipment authorizations for entities on its covered list.

Given their resource constraints and limited mandate, state and local governments should not be expected to independently grapple with the national security implications of foreign ICTS. However, they still have a responsibility to keep their own networks secure. By adhering to federal rules on foreign ICTS procurement, state and local governments can protect their digital infrastructure and keep procurement practices up to date with the latest intelligence. This may entail following mandatory ICTS rule restrictions or, if the rule is not implemented effectively, enacting policies that prevent the use of ICTS prohibited by federal agencies. Federal policymakers can

further enable state and local governments to address foreign technology threats by creating a master list of foreign ICTS covered by procurement prohibitions, strengthening existing information sharing channels, and increasing funding for rip and replace programs.

Federal policymakers now possess the authorities necessary to identify and purge untrustworthy foreign ICTS from critical U.S. networks. As they scope and implement these authorities, they should build on existing relationships with state and local officials in a shared effort to secure the country's supply chains, shore up its networks, and create space for trustworthy technology companies to innovate and grow.

## Authors

Jack Corrigan is a research analyst at CSET. Sergio Fontanez is an associate at Holland & Knight. Michael Kratsios is the managing director at Scale AI, and he previously served as the fourth chief technology officer of the United States at the White House, as well as acting under secretary of defense for research and engineering.

## Acknowledgments

For feedback and assistance, we would like to thank Catherine Aiken, Chris Chamberlain, Amy Chao, Cynthia Cook, Shelton Fitch, Conor Healy, Emily Kilcrease, Bob Kolasky, Igor Mikolic-Torreira, Nazak Nikakhtar, Dahlia Peterson, Greg Watson, Emily Weinstein, and Kevin Wolf.



Document Identifier: doi: 10.51593/20220007

## Appendix A. Data Tables

Table 3. State and Local Government Transactions Involving Covered ICTS, 2015-2021 (Including D.C.)

| State | Transactions | |
|---|---|---|
| | Value | Number |
| Alabama | $4,303 | 2 |
| Alaska | $81 | 1 |
| Arizona | $146,009 | 19 |
| Arkansas | $2,094,807 | 27 |
| California | $4,801,905 | 462 |
| Colorado | $201,972 | 31 |
| Connecticut | $73,149 | 33 |
| Delaware | $5,134 | 2 |
| District of Columbia | $0 | 0 |
| Florida | $1,930,919 | 460 |
| Georgia | $835,911 | 166 |
| Hawaii | $27,812 | 7 |

| State | Transactions | |
|---|---|---|
| | Value | Number |
| Montana | $118,328 | 46 |
| Nebraska | $71,073 | 17 |
| Nevada | $109,030 | 27 |
| New Hampshire | $44,090 | 17 |
| New Jersey | $842,951 | 228 |
| New Mexico | $213,908 | 44 |
| New York | $969,540 | 239 |
| North Carolina | $1,052,904 | 224 |
| North Dakota | $9,724 | 1 |
| Ohio | $750,607 | 251 |
| Oklahoma | $363,691 | 51 |
| Oregon | $96,365 | 38 |

| | | | | | |
|---|---|---|---|---|---|
| **Idaho** | $122,796 | 37 | **Pennsylvania** | $872,245 | 247 |
| **Illinois** | $767,994 | 211 | **Rhode Island** | $19,263 | 18 |
| **Indiana** | $101,782 | 78 | **South Carolina** | $29,179 | 12 |
| **Iowa** | $71,581 | 35 | **South Dakota** | $25,838 | 15 |
| **Kansas** | $36,206 | 26 | **Tennessee** | $404,552 | 66 |
| **Kentucky** | $61,281 | 21 | **Texas** | $6,471,374 | 886 |
| **Louisiana** | $477,297 | 151 | **Utah** | $322,644 | 21 |
| **Maine** | $80,919 | 29 | **Vermont** | $0 | 0 |
| **Maryland** | $163,264 | 48 | **Virginia** | $655,171 | 104 |
| **Massachusetts** | $536,828 | 166 | **Washington** | $1,258,139 | 372 |
| **Michigan** | $15,543,580 | 235 | **West Virginia** | $23,375 | 11 |
| **Minnesota** | $554,016 | 68 | **Wisconsin** | $1,056,221 | 196 |
| **Mississippi** | $90,826 | 34 | **Wyoming** | $4,629 | 1 |
| **Missouri** | $638,902 | 199 | | | |

Source: CSET analysis of GovSpend data.

Table 4. Annual State and Local Government Transactions Involving Covered ICTS (Including D.C.)

| Year | Transactions | |
|---|---|---|
| | Value | Number |
| **2021** | $2,181,054 | 632 |
| **2020** | $6,005,978 | 626 |
| **2019** | $5,043,153 | 1,029 |
| **2018** | $8,696,271 | 1,139 |
| **2017** | $13,505,983 | 956 |
| **2016** | $6,989,146 | 788 |
| **2015** | $2,732,533 | 510 |

Source: CSET analysis of GovSpend data.

## Appendix B. GovSpend Data Background and Methodology

Our analysis relies on data provided by GovSpend, a company that tracks federal, state, and local government procurement. To create our dataset, we first pulled all procurement records containing the words “Huawei,” “ZTE,” “Hikvision,” “Dahua,” and “Hytera” from the GovSpend database. This search returned 10,028 total transaction line items.

The authors then conducted a manual review of this data and removed line items that fell outside the scope of the analysis or lacked complete data on dates, buyers, or products. Line items were considered out of scope if they 1) occurred before 2015 or after 2021; 2) were not conducted by a state or local government entity; or 3) involved products or services that did not qualify as covered ICTS. This review resulted in the removal of 2,170 line items from our dataset. The vast majority (84 percent) of excluded transactions involved products or services that did not qualify as covered ICTS (e.g., camera mounts and brackets, battery packs, chargers, repair services, phone cases).

The remaining 7,868 purchase line items were then grouped using unique pairings of buyers and purchase-order numbers, resulting in 5,680 distinct purchase orders. Finally, the authors reviewed the organizational category of each state and local government entity within the dataset and changed the assignments for 20 entities that appeared to be miscategorized (e.g., an entity with “City School District” in its name was reclassified from “local government” to “public school”).

## Endnotes

[1] Gordon Corera, "Meng Wanzhou: The PowerPoint that sparked an international row," *BBC.com*, September 24, 2021, https://www.bbc.com/news/world-us-canada-54270739.

[2] 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.

[3] 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.

[4] National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (2017); By this time, other federal agencies had already taken steps to limit their use of certain Chinese technologies. In 2006, the U.S. Department of State stopped using computers manufactured by Lenovo on classified networks, citing the company's ties to the Chinese government. The Central Intelligence Agency and other Five Eyes intelligence agencies also allegedly banned Lenovo computers around the same time due to concerns about Chinese spying. For more, see: Grant Gross, "U.S. State Department to Limit Use of Lenovo PCs," *ComputerWorld*, May 19, 2006, https://www.computerworld.com/article/2545522/u-s--state-department-to-limit-use-of-lenovo-pcs.html; Adi Robertson, "Lenovo reportedly banned by MI6, CIA, and other spy agencies over fear of Chinese hacking (update)," *The Verge*, July 30, 2013, https://www.theverge.com/2013/7/30/4570780/lenovo-reportedly-banned-by-mi6-cia-over-chinese-hacking-fears. The DOD is prohibited from procuring certain munitions and other products and services from organizations designated as "Communist Chinese military companies" (CCMCs). This prohibition was first implemented under the 2006 NDAA and updated in 2012 and 2017, and the list of covered companies was first published by DOD in 2020. The CCMC list was retired in 2021 and replaced by the U.S. Department of the Treasury's "Chinese military-industrial complex companies" (CMIC) list. Given these changes, it is unclear whether the DOD's original procurement prohibition still applies. For more information, see: Prohibition on acquisition of certain items from Communist Chinese Military Companies 48 CFR § 225.770 (2022); "DOD Releases List of Additional Companies, in Accordance with Section 1237 of FY99 NDAA," *U.S. Department of Defense*, January 14, 2021, https://www.defense.gov/News/Releases/Release/Article/2472464/dod-releases-list-of-additional-companies-in-accordance-with-section-1237-of-fy/; "Chinese Military Company Sanctions," *U.S. Department of the Treasury*, June 3, 2021, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/topic/5671.

[5] Christopher Wray, "Open Hearing on Worldwide Threats," Testimony to the Senate Select Committee on Intelligence, 115th Congress, February 13, 2018, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats-0#.

[6] "Pentagon stops selling Huawei, ZTE phones in its bases, cites security," *Reuters*, May 2, 2018, https://www.reuters.com/article/us-usa-china-huawei-tech-idUKKBN1I326H; "Fact Sheet: Protecting

Against National Security Threats to the Communications Supply Chain Through FCC Programs," 33 FCC Rcd 4058 (2018).

[7] As noted by Adam Segal, over the last decade, policymakers in both the United States and China have begun to question whether the vulnerabilities created by interdependence in ICTS supply chains outweighed the "vulnerabilities to panopticon and choke-point threats." For more on this, see: Adam Segal, "Huawei, 5G, and Weaponized Interdependence," in *The Uses and Abuses of Weaponized Interdependence*, ed. Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, (Washington DC, Brookings Institution Press, March 2021) pg. 154.

[8] Stefan Pongratz, "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] "The 2019 A&S Top 50 Security Companies has been published and Optex ranks 24," *Optex.co*, January 24, 2020, https://www.optex.co.jp/e/news/2020/0124.html.

[10] Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, Pub. L. No. 115-232, 132 Stat. 1917 (2018).

[11] Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, 132 Stat. 5178 (2018).

[12] Executive Order No. 13873, 84 FR 22689 (2019).

[13] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 115-390, 132 Stat. 5178 (2018).

[14] 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; Samuel Woodhams, "China's Surveillance State: A Global Project," *Top10VPN*, August 3, 2021, https://www.top10vpn.com/research/huawei-china-surveillance-state/. The U.S. National Security Agency also reportedly has a history of pushing for backdoors in cryptography tools. For more, see: Kim Zetter, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA," *Wired,* September 24, 2013, https://www.wired.com/2013/09/nsa-backdoor/.

[15] 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; "Hikvision Backdoor Exploit," *IPVM*, September 3, 2017, https://ipvm.com/reports/hik-exploit; Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *The Wall Street Journal*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

[16] Ellen Nakashima and Aaron Schaffer, "Chinese hackers compromise dozens of government agencies, defense contractors," *The Washington Post*, April 21, 2021, https://www.washingtonpost.com/national-security/chinese-hackers-compromise-defense-contractors-agencies/2021/04/20/10772f9e-a207-11eb-a7ee-949c574a09ac_story.html; Corin Faife, "China backed hackers breached government networks in at least six US states, per new report," *The Verge,* March 8, 2022, https://www.theverge.com/2022/3/8/22966517/china-hack-government-networks-apt41-usaherd.

[17] 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.

[18] 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.

[19] "Hikvision USA Declares 'HERETOSTAY,' With ADI," *IPVM*, April 21, 2022, https://ipvm.com/reports/hik-usa-stay.

[20] The CCP has long used subsidies, export financing, and other measures to drive down the cost of Chinese technologies, making them more competitive in the global market. This financial support was critical to Huawei's rise as a global telecommunications giant. For more, see: Rubin et al., "The Huawei Moment." For a discussion of the impact of Chinese government subsidies in the semiconductor industry, see: Stephen Ezell, "Moore's Law Under Attack: The Impact of China's Policies on Global Semiconductor Innovation" (Information Technology and Innovation Foundation, 2021), https://itif.org/publications/2021/02/18/moores-law-under-attack-impact-chinas-policies-global-semiconductor/.

[21] We compared the Hikvision DS-2CE56D7T-AITZ ($90) to Hanwha HCD-6070R ($190), March Networks 35835-101 ($290), and the Panasonic WV-U2132L ($431) on Amazon.com as of August 2022. "Equivalent" cameras were selected using the BestMatch tool developed by IPVM, a surveillance industry observer.

[22] Joseph Marks, "Amid a surge in ransomware attacks, cities are taking some of the biggest hits," *The Washington Post*, September 3, 2021, https://www.washingtonpost.com/politics/amid-a-surge-in-ransomware-attacks-cities-are-takingsome-ofthe-biggest-hits/2021/09/02/9bd5d654-0a84-11ec-aea1-42a8138f132a_story.html.

[23] Richard Forno, "Local Governments Are Attractive Targets for Hackers and Are Ill-Prepared," *Governing.com*, March 29, 2022, https://www.governing.com/now/local-governments-are-attractive-targets-for-hackers-and-are-ill-prepared.

[24] Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, Pub. L. No. 115-232, 132 Stat. 1917 (2018); Executive Order No. 13873, 84 FR 22689 (2019).

[25] *Information Technology: Digital Service Programs Need to Consistently Coordinate on Developing Guidance for Agencies* (Washington, DC; Government Accountability Office, 2021), *https*://www.gao.gov/assets/gao-22-104492.pdf#page=6.

[26] "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; "The 2019 A&S Top 50 Security Companies has been published and Optex ranks 24," *Optex.co*, January 24, 2020, https://www.optex.co.jp/e/news/2020/0124.html.

[27] Brandi Vincent, "Security Firm Says Huawei, ZTE Devices Still Run on Government Networks," *Nextgov*, May 30, 2019, https://www.nextgov.com/cybersecurity/2019/05/security-firm-says-huawei-zte-devices-still-run-government-networks/157370/; Sheridan Prasso, "China Tech's Grip Persists in US Long After Orders to Rip It Out," *Bloomberg*, May 11, 2022, https://www.bloomberg.com/news/articles/2022-05-11/us-ban-on-china-tech-failed-to-stop-use-of-hauwei-zte-hardware; Asa Fitch, "U.S. Government Still Uses Suspect Chinese Cameras," *The Wall Street Journal*, October 19, 2019, https://www.wsj.com/articles/u-s-government-still-uses-suspect-chinese-cameras-11571486400.

[28] At the time the law was passed, lawmakers provided few details on why certain companies were covered by the regulation and others were not. U.S. officials had long painted Huawei and ZTE as security threats, but Hikvision, Dahua, and Hytera had generally not faced the same level of criticism.

[29] Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment, 48 CFR § 52.204-24; Sam Biddle, "U.S. Military Bought Cameras In Violation of America's Own China Sanctions," *The Intercept*, July 20, 2021, https://theintercept.com/2021/07/20/video-surveillance-cameras-us-military-china-sanctions/; Federal Acquisition Regulation; Federal Acquisition Circular 2020-08; Introduction, 85 FR 42664 (2020).

[30] Section 889 originally gave contractors until August 13, 2020 to remove covered ICTS from their networks, but the DOD and U.S. Agency for International Development have been allowed to continue working with vendors that use covered equipment through September 30, 2022. The DOD waiver specifically applied to vendors providing "low risk" items such as food, transportation, and medical care. For more, see: Director of National Intelligence, *Department of Defense Request for Waiver of Section 889 of Fiscal Year 2019 National Defense Authorization Act*, John Ratcliffe, https://thecgp.org/images/Memo-20-00823_DoD-Request-for-Section-889-Waiver-2.pdf; For more on the USAID waiver, see: USAID Industry Liason, *Information on USAID's Section 889 Telecommunications Waiver*, https://federalnewsnetwork.com/wp-content/uploads/2020/10/including-USAID.pdf.

[31] 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/.

[32] Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, 132 Stat. 5178 (2018).

[33] The provision defines "supply chain risk" as "the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of the covered articles or information stored or transmitted on the covered articles." For more, see: Authorities related to mitigating supply chain risks in the procurement of covered articles, 41, U.S. Code § 4713 (2022).

[34] The FASC was also tasked with developing supply chain risk management standards alongside the National Institute of Standards and Technology (NIST) and assisting federal agencies and other public and private organizations in adopting those standards.

[35] At the time of the FASC's creation, the government was engaged in a protracted legal battle with the Russian cybersecurity firm Kaspersky Lab over a Department of Homeland Security (DHS) order banning 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 FASC process avoids this issue, requiring policymakers to justify their actions against particular vendors and giving companies the chance to respond. 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/. For more on the FASC's recent actions, see: "Federal Acquisition Regulation (FAR); FAR Case 2020-011, Implementation of FASC Exclusion Orders," Office of Information and Regulatory Affairs, Spring 2022, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202204&RIN=9000-AO13.

[36] The Director of National Intelligence is authorized to issue orders to the intelligence community, the Secretary of Defense is authorized to issue orders to the Department of Defense, and the Secretary of Homeland Security is authorized to issue orders to civilian agencies: Federal Acquisition Security Council, "Federal Acquisition Security Council Rule," *Federal Register* 86, no. 163 (August 26, 2021): 47581-47593, https://www.govinfo.gov/content/pkg/FR-2021-08-26/pdf/2021-17532.pdf.

[37] Executive Order 13873 defines transaction as "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service." For more, see: Securing the Information and Communications Technology and Services Supply Chain, 86 FR 4909 (2021).

[38] *CFIUS Summary Data 2008-2020*, (Washington, DC; Department of the Treasury), https://home.treasury.gov/system/files/206/CFIUS-Summary-Data-2008-2020.pdf#page=2.

[39] *Securing the Information and Communications Technology and Services Supply Chain: Regulatory Impact Analysis & Final Regulatory Flexibility Analysis*, (Washington, DC; Department of Commerce, 2021), https://www.regulations.gov/document/DOC-2019-0005-0074. In March 2021, the Commerce Department subpoenaed multiple Chinese companies as part of an effort to investigate whether the firms "meet the criteria set forth in" the ICTS rule.

[40] *The Department of Commerce Budget in Brief: Fiscal Year 2023*, (Washington, DC: Department of Commerce, 2022), https://www.commerce.gov/sites/default/files/2022-03/Commerce-FY2023-BIB-Introduction.pdf#page=74.

[41] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020).

[42] "List of Equipment and Services Covered by Section 2 of The Secure Networks Act," *U.S. Federal Communications Commission*, September 20, 2022, https://www.fcc.gov/supplychain/coveredlist. The law specifically calls on commissioners to update the list to reflect determinations made by the FASC and Commerce Department.

[43] Funding would be made available to providers with fewer than 2 million customers.

[44] Igor Bonifacic, "US carriers ask the FCC for $5.6 billion to replace Huawei and ZTE Equipment," *Engadget,* February 6, 2022, https://www.engadget.com/fcc-huawei-zte-rip-replace-funding-211116669.html.

[45] The House Energy and Commerce Committee approved a bill to cover the funding shortfall. See: Christopher Cole, "House Panel Advances 'Rip and Replace' Shortfall Fix," *Law360*, June 15, 2022, https://www.law360.com/articles/1502739/house-panel-advances-rip-and-replace-shortfall-fix.

[46] Margaret Harding McGill, Bethany Allen-Ebrahimiam, and Jonathan Swan, "FCC poised to ban all U.S. sales of new Huawei and ZTE equipment," *Axios*, October 13, 2022, https://www.axios.com/2022/10/13/fcc-ban-huawei-zte-equipment.

[47] The notice of proposed rulemaking also suggested commissioners are considering revoking existing authorizations of covered ICTS. For more, see: U.S. Federal Communications Commission, "FCC Proposes Ban on Equipment Authorizations for Devices Deemed to Pose a Threat to National Security," U.S. Federal Communications Commission, June 17, 2021, https://docs.fcc.gov/public/attachments/DOC-373363A1.pdf.

[48] Rufus Brown, Van Ta, Douglas Bienstock, Geoff Ackerman, John Wolfram, "Does This Look Infected? A Summary of APT41 Targeting U.S. State Governments," *Mandiant*, March 8, 2022, https://www.mandiant.com/resources/apt41-us-state-governments; Andy Greenberg, "Chinese Hacking Spree Hit an 'Astronomical' Number of Victims," *Wired,* March 5, 2021, https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/.

[49] Katie Bo Lillis, "CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could distrupt 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.

[50] These figures are based on the total retail value of the equipment and services purchased. They do not account for any discounts or reimbursements the procuring organization may have received, and exclude purchases of corporate subsidiaries, such as Lorex.

[51] The CCP has long used subsidies, export financing, and other measures to drive down the cost of Chinese technologies, making them more competitive in the global market. This financial support was critical to Huawei's rise as a global telecommunications giant.

[52] The New York and Florida state legislatures also proposed bills aimed at combating Chinese technology threats, but in both cases these measures died in committee. The New York bill, known as SB-7584, would have implemented the same three prohibitions as Section 889: barring state agencies from purchasing ICTS from Huawei, ZTE, Hikvision, Dahua, and Hytera; forbidding state agencies from working with vendors that use covered ICTS; and preventing government funds from being used to purchase this equipment. For more, see: New York S07584, 2020 Legislative Session (2020). The Florida bill, known as SB-810, would have barred state agencies and local government entities from purchasing any product in which more than 25 percent of the components were produced in China, as well as all procurements from Facebook, Twitter, Alphabet, Apple, and Amazon. For more, see: Prohibited Governmental Transactions Involving Certain Companies and Products, Florida S.B. 810 S07584, 2021 Legislative Session (2021).

[53] Procurement of telecommunications or video surveillance equipment or services by agencies or certain educational entities, La. Stat. tit. 38 § 2237.1 (2021).

[54] Department of Administrative Services; companies owned or operated by China to bid on or submit a proposal for a state contract; prohibit, Georgia S.B. 346, 2021-2022 Regular Session (2022); Georgia also enacted an identical law prohibiting companies owned and operated by the Russian and Belorussian governments from applying for state contracts. The measure, S.B. 562, was signed into law the same day as S.B. 346.

[55] Dozens of Chinese state-owned enterprises are already included on the Bureau of Industry and Security's Entity List, which generally prohibits U.S. individuals, companies, and government entities from exporting to them.

[56] Agency of Digital Services, *Cybersecurity Standard Update 19-01*, John Quinn, https://s3.documentcloud.org/documents/5744806/ADS-Cybersecurity-Directive-19-01.pdf.

[57] According to the order, these threat determinations can be based on documentation from "any government agency, cybersecurity firm, or expert." See: Office of the Governor, *Executive Order Number 22-216: Strengthening Florida Cybersecurity Against Foreign Adversaries*, Ron DeSantis, https://www.flgov.com/wp-content/uploads/2022/09/Executive-Order-22-216.pdf.

[58] Foreign gifts and contracts, Fla. Stat. § 286.101 (2022).

[59] Bureau of Industry and Security, *Fiscal Year 2022 President's Budget Submission* (Washington, DC; U.S. Department of Commerce, 2021), https://www.commerce.gov/sites/default/files/2021-06/fy2022_bis_congressional_budget_justification.pdf; *The Department of Commerce Budget in Brief: Fiscal Year 2023*, (Washington, DC: Department of Commerce, 2022), https://www.commerce.gov/sites/default/files/2022-03/Commerce-FY2023-BIB-Introduction.pdf#page=74.

[60] Ibid.

[61] Emily Kilcrease, "Using a Sanctions Framework to Fix the ICTS Executive Order," *Lawfare*, December 17, 2021, https://www.lawfareblog.com/using-sanctions-framework-fix-icts-executive-order.

[62] Ibid.

[63] *Securing the Information and Communications Technology and Services Supply Chain: Regulatory Impact Analysis & Final Regulatory Flexibility Analysis*, (Washington, DC; Department of Commerce, 2021), https://www.regulations.gov/document/DOC-2019-0005-0074.

[64] Kilcrease, "Using a Sanctions Framework to Fix the ICTS Executive Order."

[65] Secure Equipment Act of 2021, Pub. L. No. 117-55, 135 Stat. 423 (2021).

[66] Margaret Harding McGill, Bethany Allen-Ebrahimiam, and Jonathan Swan, "FCC poised to ban all U.S. sales of new Huawei and ZTE equipment," *Axios*, October 13, 2022, https://www.axios.com/2022/10/13/fcc-ban-huawei-zte-equipment.

[67] In a recent brief, the National Governors Association called on state policymakers to change procurement rules and other risk management policies to defend against foreign technology threats in the energy infrastructure sector. For more, see: *Issue Brief: States' Role in Foreign Threats in U.S. Energy Critical Infrastructure Sectors*, (Washington, DC; National Governors Association, 2022), https://www.nga.org/wp-content/uploads/2022/01/NGA-Foreign-Influence-Energy-Infrastructure_Jan2022.pdf.

[68] Benjamin Freed, "CISA director offers governors advice on talking about cyber," *StateScoop*, January 31, 2022, https://statescoop.com/cisa-jen-easterly-national-governors-association/;

[69] Mol Doak, "What is the State of Ransomware Threats for State and Local Agencies?" *StateTech*, March 1, 2022, https://statetechmagazine.com/article/2022/03/what-state-ransomware-threats-state-and-local-agencies.

[70] Joseph Marks, "A 2020 ransomware attack is still harming Baltimore teachers," *The Washington Post*, April 18, 2022, https://www.washingtonpost.com/politics/2022/04/18/2020-ransomware-attack-is-still-harming-baltimore-teachers/; Lily Hay Newman, "The Ransomware that Hobbled Atlanta Will Strike Again," *Wired*, March 30, 2018, https://www.wired.com/story/atlanta-ransomware-samsam-will-strike-again/.

[71] *Secure and Trusted Communications Networks Reimbursement Program: Frequently Asked Questions* (Washington, DC; Congressional Research Service, 2022), https://crsreports.congress.gov/product/pdf/IN/IN11663.

[72] "List of Equipment and Services Covered by Section 2 of The Secure Networks Act," *U.S. Federal Communications Commission*, September 20, 2022, https://www.fcc.gov/supplychain/coveredlist.

[73] Tate Ryan-Mosley, "The world is moving closer to a new cold war fought with authoritarian tech," *MIT Technology Review*, September 22, 2022, https://www.technologyreview.com/2022/09/22/1059823/cold-war-authoritarian-tech-china-iran-sco/.