SECURE EQUIPMENT: THE WHOLE OF GOVERNMENT EFFORT TO RESTRICT DANGEROUS DEVICES

Cyberattacks against the United States occur with increasing sophistication, frequency, and severity. Attacks are pervasive on critical infrastructure, government agencies, financial institutions, enterprises, and individuals. While U.S. defenses have largely focused on software vulnerabilities, hardware attacks can be harder to deter and can cause greater damage. A highly vulnerable attack surface is the mass of electronic equipment produced by companies owned and affiliated by the People's Republic of China (PRC). Information technology products and services from the PRC can facilitate cyber intrusion for the conduct of theft, surveillance, sabotage, and warfare against the United States.

In response, federal policymakers have begun to focus U.S. cyber-defense strategies on hardware and network security—and rightly so. In November 2021, the Secure Equipment Act became law, which authorizes the Federal Communications Commission (FCC) to restrict equipment authorizations through the agency's "Covered Equipment or Services List" (Covered List). Expanding the Covered List will allow the FCC to restrict authorizations for equipment made by companies with ties to the PRC and the People's Liberation Army (PLA) from entering U.S. markets and sensitive networks.

The Secure Equipment Act marks a critical step to consolidate consumer protections with defense and strategic trade instruments, like the National Defense Authorization Act (NDAA) and the U.S. Entity List. To date, inconsistent controls have allowed consumers and state/local governments to continue to purchase and install vulnerable and insecure equipment from the PRC. The Secure Equipment Act closes loopholes which allowed continued equipment authorizations for Covered List companies like Huawei, ZTE, Dahua, Hikvision, and Hytera. These are entities which U.S. national security authorities have identified as presenting unacceptable risks to national security and therefore must be restricted.

Today just five companies are named on the FCC's Covered List. FCC Commission Brendan Carr suggests that drone maker DJI be added, based upon the national security assessment and its practice of collecting Americans' personal information for processing in the PRC.

There are literally hundreds, if not, thousands of PRC companies providing information technology products and services in the USA. China Tech Threat proposes a rational process to add additional entities to the Covered List because of their ownership and affiliation to the PRC and the associated national security risk.

China Tech Threat supported the adoption of the Secure Equipment Act. This briefing paper summarizes these activities. Further, it explores the U.S. government's recognition of the unacceptable national security risk of equipment made by companies in the PRC and the FCC's role in risk mitigation. It describes two such entities, Lenovo and Yangtze Memory Technologies Company (YMTC), as specific examples of companies that should be added to the FCC's Covered List.

Filings to the FCC Comments Submitted with BluePath Labs

Event with FCC Commissioner Brendan Carr, CNAS, CSET and TIA

Letter to Congress Commending Secure Equipment Act of 2021

Multiple Writings on the Issue, Including a Published Piece in Forbes

The FCC's Role in Secure Networks and Equipment: Ending Authorization for Equipment With Poses Unacceptable National Security Risk

The Secure and Trusted Networks Act of 2019 authorized the FCC to place telecommunications equipment and services on the Covered List based on a determination by U.S. national security agencies.

The law recognized that certain policy instruments enacted by federal agencies do not necessarily translate to protections for and controls on equipment and services at the consumer or end-user level. It therefore provides a blueprint for the FCC to restrict equipment as necessary to achieve the latter.

The bipartisan, bicameral Secure Equipment Act of 2021 bolstered the 2019 legislation and provides clarification and support for the FCC to conduct these tasks. It also seeks to empower the FCC to adopt rules to restrict equipment authorizations to companies on the agency's Covered List.

The 2021 legislation was introduced by Senators Marco Rubio (R-FL) and Ed Markey (D-MA), Congresswoman Anna Eshoo (D-CA), and Minority Whip Steve Scalise (R-LA), and it was co-sponsored by 22 members in the House of Representatives from both sides of the political aisle. The bill passed in the House by an overwhelming 420-4 vote on October 28, 2021. Eight days later, it was passed in the Senate by unanimous consent, and President Biden signed it into law on November 12, 2021.

"[This] bipartisan legislation will keep compromised equipment out of U.S. telecommunications networks and ensure our technology is safe for consumers and secure for the United States," Senator Markey said.

"This legislation adds an extra layer of security that slams the door on entities that pose a national security risk from having a presence in the U.S. telecommunications network," said Representative Scalise. "Equipment made by Huawei and ZTE, companies linked to the Chinese government, increases the vulnerabilities of our telecommunication systems and puts our national security at risk. Our bipartisan, bicameral bill prohibits the FCC from issuing licenses for any telecommunications equipment made by Huawei or ZTE."

Numerous federal agencies, including the Office of the Director of National Intelligence, the Department of Justice, the National Security Agency, and the Federal Bureau of Investigation, have warned that PRC state-sponsored cyber actors aggressively target U.S. assets—notably those with high political, military, economic, infrastructure, and personnel and/or organizational value.

The purpose of these attacks is to steal sensitive data, emerging technologies, intellectual property, and personally identifiable information (PII), and to identify and exploit vulnerabilities in U.S. networks.

America's growing installation of electronics equipment and devices manufactured by PRC state-owned and military-aligned firms represents another playing field for the PRC to conduct theft, surveillance, espionage, sabotage, and warfare against the United States. Threats from PRC information technology products and services include the presence of malicious hardware, software, and components; data theft and exfiltration; and unethical and illegal business practices in the development, production, and distribution of these products and services.

China's Strategy of Military Civil Fusion Permeates Its Technology Sector

In September 2021, China Tech Threat and BluePath Labs submitted a comment following the FCC's notice of proposed rulemaking related to the agency's equipment authorization program (ET Docket No. 21-232) and competitive bidding process (ET Docket 21-233). This input noted that as part of its Military-Civil Fusion Strategy, the PRC "is engaged in a committed, long-term plan to displace the U.S. in military and economic leadership, and information technology is a key front for this offensive." The filing demonstrated that per the 2019 Secure and Trusted Networks Act, Lenovo and Yangtze Memory Technologies Company (YMTC) should be added to the FCC's Covered List for restriction on equipment authorization.

The PRC industrial policy strategy, Made in China 2025 [中国制造 2025], and the Dual Circulation [国内国际双循环] policy, launched in 2015 and 2020 respectively complement its Five-Year plans, and are intended to bolster the PRC's overall economic strength while promoting technological innovation and reducing reliance on foreign technology [1]. In doing so it seeks to displace the U.S.'s and other countries' leading position. These policies have come into even sharper focus as the PRC continues to rely on semiconductors to an outsize degree--making breakthroughs in that technology by any and all means a major priority.

Information technology is a pillar of the displacement strategy, as described as techno nationalization or techno globalization. The PRC is the only threat actor which has an IT industry which rivals America's. Chinese computers, devices, software, and other information technologies are ubiquitous and embedded with PRC government practices and laws which may facilitate intrusion, theft, espionage, surveillance, sabotage, or other compromise of integrity. These practices can also be described as a form of cyberwarfare.

The PRC is actively working to improve the efficiencies of its research and infrastructure investments in both the civilian and military spheres, what it describes as its Military-Civil Fusion Strategy [军民融合战略], hereafter MCFS. MCFS seeks to acquire, exploit, and weaponize American-made technologies and, ultimately, usurp the United States' economic and military leadership. The PRC is engaged in a sustained, whole-of-nation campaign of cyber-warfare against the United States that seeks to disrupt U.S. networks and acquire sensitive technologies that can be used against American national security and economic interests [2] As of 2018, at least 3,000 PRC enterprises participate in MCFS, with 70 percent coming from the IT industry [3].

All PRC information technology is vulnerable to PRC intrusion, whether through technical means like control channels, backdoors, or kill switches, or through government practices of surveillance, espionage, and sabotage. The only way to effectively mitigate the risk of PRC intrusion is to restrict the devices and equipment.

Consequently, the PRC's enormous global market position in the IT manufacturing market gives it many long-term advantages to conduct infiltration (it has the knowledge and blueprints of its products), supply chain attacks (embedding malware in products), human intelligence (learning about customers, participating in U.S. trade associations), and social engineering. Supply chains are vulnerable to threats that may turn out to be more significant in the long term: Chips could be intentionally compromised during the design process before they are even manufactured.

If placed into the design with sufficient skill, these built-in vulnerabilities would be extremely difficult to detect during testing. And they could be exploited months or years later to disrupt or exfiltrate data from a system containing the compromised chip.

The U.S.-China Economic and Security Review Commission's (USCC) 2018 "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology" report concluded that Lenovo is in the same class as Huawei and ZTE for its proximity to the PRC government [4]. "Huawei, Zhongxing Telecommunications Corporation (ZTE), and Lenovo are three Chinese ICT companies that exhibit some of these characteristics...Lenovo's growth has been attributed to the economic and political support it receives from the Chinese government, including the use of state-owned intellectual property resources. Lenovo has been linked to Chinese state-led cyberespionage efforts. Lenovo products have been banned by intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the United States (Five Eyes Countries) since the mid-2000s, when laboratories of the British intelligence agencies Military Intelligence, Section 5 and Government Communications Headquarters discovered 'backdoors' and vulnerable firmware in Lenovo products." [5] Indeed Lenovo may be a graver concern because it facilitates the process and storage of data on laptops and servers, unlike Huawei and ZTE which enable primarily transmission, frequently of encrypted data.

Importantly the FCC recognizes that the equipment authorization responsibility may be held by more than the equipment manufacturer. It recognizes, "... the assembler (if the equipment is assembled from individual component parts and the resulting system is subject to authorization), or the importer (if the equipment by itself or the assembled system is subject to authorization) and could also include retailers and parties performing modification under certain circumstances." As such, the FCC is mindful that regulating the brand name on the package is not sufficient to ensure security.

YMTC provides an important example of a producer of key component in electronic equipment (semiconductors) which presents national security risk. Among other dangers, YMTC chips can be enabled with kill switches which can cause a device and/or network shutdown. As explained in the 2021 White House 100 Day Supply Chain Report, YMTC is "emerging as China's national champion memory chip producer" and "represents a watershed moment in China's semiconductor ambitions [6]."

The report also notes that while it was "only [emphasis added] founded in July 2016," it "received an estimated $24 billion in subsidies from Chinese government sources, which was essential to the firm's rapid development." Additionally, YMTC and the PRC's use of subsidy, espionage, and anticompetitive and illegal practices to support it are detailed by Chinese military expert James Mulvenon [7].

Given that the Department of Commerce's Bureau of Industry and Security (BIS) placed Fujian Jinhua on the Entity List and designated Semiconductor Manufacturing International Corporation (SMIC) as a Military End User, it was widely expected in 2020 that YMTC would be next. BIS' delay in taking this needed action has resulted in censure by Congress [8]. It has been suggested that given their growing and record profits in the PRC, U.S. semiconductor manufacturing equipment makers Applied Materials, KLA, and Lam Research have succeeded to deter BIS from designating YMTC for its national security risks[9]. As such, China Tech Threat recommends that the FCC's prohibit equipment authorizations containing chips from Yangtze Memory Technologies Company (YMTC).

Expanding the Covered List: A Mandate from Congress

Most Americans don't realize that they are at risk from intrusion by PRC actors when they use products and services from Covered List entities—many of which are widely available through Amazon, Best Buy, Walmart, and other major retailers. Despite major policies enacted by the Congress, the Department of Defense, and the Department of Commerce to address risks posed by these entities, the FCC reports that some 3,000 applications for equipment authorization from Huawei alone have been approved since 2018.

Congress' passage of the Secure Equipment Act reaffirms the United State's commitment to core shared values:

- Rule of Law: The FCC was chartered by the Communications Act of 1934 with the express purpose for the safety and security of communication, ensuring "adequate facilities at reasonable charges, for the purpose of the national defense, for the purpose of promoting safety of life and property through the use of wire and radio communication…" The passage of the Secure Equipment Act demonstrates that Congress plays an essential role in clarifying the FCC's authority so that regulation is not under or over interpreted.

- Defense: The Secure Equipment Act demonstrates a recognition that national defense is a mandatory function of government. The unacceptable levels of theft of intellectual property via communications networks, data breach, and other forms of unauthorized access of Americans' information technology by the PRC is effectively cyber war. The bill mandates meaningful action to reduce Americans' exposure to malicious Covered List providers of information technology.

- Competition: Equipment authorization is a privilege, not a right, for lawful providers that honor America's laws. Many PRC entities have engaged in theft, predatory pricing, and other anticompetitive practices to gain market share. These monopolies encompass once competitive markets for certain categories of computers, smartphones, communications equipment, solar panels, flat panel displays, and light emitting diodes (LED). There are dozens of non-PRC equipment providers that struggle to gain a foothold in the market because of unfair and unlawful practices by PRC firms. Restricting unlawful firms will open and level the playing field for companies operating within the bounds of U.S. law.

FCC Covered List: Mitigating Unacceptable Risk to U.S. National Security

Even prior to Congress' approval of the Secure Equipment Act, the FCC had begun proceedings to close loopholes that allowed PRC associated companies to sell products in U.S. markets. In September 2021, the FCC issued a notice of proposed rulemaking (NPRM) that sought to prohibit future authorizations for communications equipment made by entities that pose unacceptable risk to U.S. national security. The NPRM also sought input about whether equipment authorizations should be retroactively revoked for equipment made by companies with known ties to foreign adversaries.

The FCC has a unique, important authority granted by Congress to regulate commercial equipment that uses radio frequencies and has made a good start to propose prohibiting equipment authorizations from entities on the Covered List—which currently include five Chinese military aligned companies (Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company).

On October 20, 2021, FCC Commissioner Brendan Carr announced at a China Tech Threat event that the agency had commenced a process to add SZ DJI Technology Company (DJI), the world's largest drone maker, to the FCC's Covered List. DJI controls about 50 percent of the U.S. drone market and 70 percent of the global consumer and enterprise drone market [10].

"DJI is 'Huawei on wings,'" Commissioner Carr said. "Most people don't understand the vast amounts of information being collected by drones."

However, there are many more PRC associated entities operating in the United States, which pose an unacceptable national security risk. The FCC's expansion of the Covered List will better apply these prohibitions to all PRC state-owned and military-aligned entities that operate in the United States. In a letter to Congress, China Tech Threat and more than 20 other organizations and industry leaders noted:

- "There are many other PRC entities making products, services, and components which pose an unacceptable national security risk to Americans and which should be considered for Covered List addition; these include but are not limited to the Yangtze Memory Technologies Corp (YMTC), Lenovo, and TikTok. We encourage the FCC to follow the path outlined by 2019 Secure and Trusted Networks Act, which identifies entities to be placed on Covered List."

Not surprisingly, some U.S. companies and industry representatives have opposed the FCC's proposal to restrict equipment authorizations. While some concerns are legitimate, the following points reiterate the importance that the FCC proceed with its proposed rulemaking.

Selling Electronic Equipment Is a Privilege, Not a Right

Some petitioners have opposed elements of the NPRM on grounds that the proposed regulations would disrupt enterprise. While prohibiting future authorizations for Covered List entities may disrupt some revenue for some providers, equipment authorization is a privilege, not a right, for entities that uphold U.S. laws.

The purpose of the Communications Act is not to maximize revenue for firms, even though tens of thousands of firms have earned revenue through the FCC's equipment authorization regime. The purpose of the Communications Act is to promote the safety and life of property through wire and radio communication.

Yet, the FCC's equipment authorization program is being abused by foreign entities with unacceptable levels of national security risk. Not only do these entities profit from the FCC's program, current rules also allow vulnerable equipment to be marketed and installed across the United States. This puts millions of Americans at risk for intrusion by PRC actors and endangers Americans' security, privacy, and property.

Given the facts and determinations by relevant national security agencies, the FCC must act to mitigate this risk. In fact, the FCC would be irresponsible if it continued to authorize equipment to entities it knows present unacceptable national security risk.

Level the Playing Field for Lawful Equipment Makers

All equipment providers pose some level of risk. The purpose of the FCC proceeding is to restrict actors with unacceptable risk. In so doing, the FCC will strengthen and even the playing field for lawful providers with acceptable risk.

As noted above, the PRC state-owned and military-aligned entities have engaged in intellectual property theft, predatory pricing, and other anticompetitive practices to achieve an advantage in U.S. and global markets. This has created barriers to entry and other distortions. The Coalition for a Prosperous America noted in public comment:

- "The preponderance of PRC manufacturers like the entities on the Covered List create significant barriers to entry in the electronic equipment market. Manufacturers from other nations are crowded out by heavily-subsidized PRC companies with a series of illegal practices, including, but not limited to, forced/slave labor, theft, product dumping, predatory pricing, currency manipulation, forced tech transfer, and so on… The aggressive behavior and predatory pricing of Huawei and ZTE has forced U.S. networking equipment vendors out of the market. Today, the U.S. has no vendor capable of providing a complete end-to-end wireline or wireless network."

One of the goals of the FCC's equipment authorization program is to promote competition through an efficient, transparent, and rules-based system. Without FCC intervention, certain categories of electronic equipment could become monopolized by PRC vendors.

Only Covered List Entities Should Be Subjected to Additional Obligations

The idea that the FCC should refuse to address recognized national security concerns because it could upset a company's revenue stream is not justified. It is not the job of the FCC to maximize revenue for firms. However, additional regulatory burdens should be relegated to entities identified by the Covered List, especially in light of the often razor-thin margins equipment makers face.

Accordingly, increased obligations should not be applied to the entire industry, only to those entities that are added to the Covered List. As such, the legitimate playing field for lawful equipment providers would be preserved, if not strengthened.

China Tech Threat supports the proposed regulation for Covered List entities, provided that the List is expanded appropriately. The Commission has acknowledged that the proposed regulations amount to a significant intervention and endeavors to minimize the regulatory burden. At the same time, the ease of the current equipment authorization process allows the risk of equipment with unacceptable national security risks to go unchecked. The current process is not sufficiently rigorous to weed out risky suppliers and equipment.

Regulation Should Focus on Future Prohibitions

There is a wealth of equipment already in the U.S. market the poses a threat to national security. The FCC observes, for example, that at least 3,000 equipment authorizations have been granted to Huawei alone since 2018. However, there is legitimacy to claims that retroactively revoking equipment authorizations could unduly burden manufacturers acting in good faith and disrupt supply chains.

It is reasonable for the FCC to prohibit future authorizations while leaving past authorizations in place. This would allow time for the FCC to communicate to the public on a going-forward basis. Notably, many previously approved devices from Covered List entities will be ripped and replaced in the normal course of use.

China Tech Threat finds it reasonable that the FCC need not revoke past authorizations if by going forward it restricts equipment authorizations to Covered List entities and adds new entities as appropriate.

A Clear, Distinct Mandate from Congress to Close a Loophole

The FCC's proposed regulations do not duplicate or disrupt other federal cybersecurity obligations, which some industry voices raised as a reason to oppose the proposed rules. While it is true that there are many federal cybersecurity rules, none of these existing rules effectively address or mitigate the unacceptable risk of installed electronic equipment using radio frequencies. In general, federal policy is overly weighted to software, not hardware, risk. This itself is a policy blind spot and a reason FCC action is justified.

The proposed regulation reflects a clear, distinct mandate from Congress to the FCC, as it seeks to close loopholes in the NDAA and Entity List designations. As Commissioner Carr explained, the proposed rules "would close a glaring loophole that Huawei and others are exploiting today to place their insecure gear into our networks."

While some industry advocates have called for a national "unified framework" for cybersecurity, that is the job of Congress to develop and implement—not the FCC. With its proposed rulemaking, the FCC is doing exactly what Congress instructs it to do based upon its authority from the 1934 Communications Act.

Conclusion

As cyber-threats against the United States continue to escalate and evolve, it is critical that policymakers address the glaring threat from equipment made by companies with ties to the PRC. Congress' approval of the Secure Equipment Act demonstrates that federal authorities recognize this growing threat sector and have begun to restructure U.S. defenses to better protect the "whole of society."

The FCC Covered List is one of the few tools that bridges the gaps between the patchwork of federal restrictions. As such, the agency's proposals to tighten equipment authorizations is a logical and indeed necessary step to stop the PRC and other bad actors from spying and collecting data on Americans, and could very well prevent a catastrophic attack against critical U.S. networks.

While some U.S. companies may oppose these measures, which could disrupt their short-term revenues, it is imperative that the FCC fulfill its mandate from Congress by prudently expanding the Covered List to include companies that pose an unacceptable risk to U.S. national security. What's more, the FCC should consider targeting key technologies, like semiconductors and semiconductor manufacturing equipment, to better protect U.S. interests and foster greater competition.

Countering the PRC's cyber-threat will require greater scrutiny of technology that has long been allowed to permeate U.S. markets. The Secure Equipment Act and the FCC's proposed strengthening of the Covered List are important and welcome progress to address major security risks in electronic equipment. It is imperative that these efforts not be derailed by industry interests that would put short-term gains ahead of long-term security.

Endnotes

[1] Alicia García Herrero, "What is Behind PRC's Dual Circulation Strategy" PRC Leadership Monitor, Fall 2021 Issue 69 1 September 2021. https://3c8314d6-0996-4a21-9f8a-

[2] Stone, Alex, and Peter Wood. "PRC's Military-Civil Fusion Strategy: A View from Chinese Strategists." (2020). https://www.bluepathlabs.com/uploads/1/1/9/0/119002711/PRCs_military_civil_fusion_strategy-_full_final.pdf

[3] "Roughly 3,000 Private Chinese Enterprises Have Entered the Front Line of Military Industrial Procurement" [我国大约3000家民企已进入军工采购一线], Xinhua, 14 March 2018, http://m.xinhuanet.com/mil/2018-03/14/c_129829001.htm.

[4] "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology." USCC April 19, 2018. https://www.uscc.gov/research/supply-chain-vulnerabilities-china-us-federal-information-and-communications-technology.

[5] Ibid.

[6] "Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-Based Growth." The White House. June 2021. https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

[7] "China Aims to Dominate Flash Memory – SOSi's Dr. James Mulvenon Quoted." SOSI. January 4, 2021. https://www.sosi.com/news/china-aims-to-dominate-flash-memory/

[8] "McCaul, Hagerty Urge Raimondo to Include the CCP's YMTC on Commerce Department Entity List". Press Release, GOP Foreign Affairs Committee. July 12, 2021. https://gop-foreignaffairs.house.gov/press-release/mccaul-hagerty-urge-raimondo-to-include-the-ccps-ymtc-on-commerce-department-entity-list/

[9] Robert Castellano. "Applied Materials And Lam Research: Little Impact From Possible Demise Of China's NAND Industry." Seeking Alpha. July 19, 2021. https://seekingalpha.com/article/4439969-applied-materials-and-lam-research-little-impact-from-possible-demise-of-chinas-nand-industry

[10] https://chinatechthreat.com/fcc-commissioner-dji-is-huawei-on-wings/