Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

REPLY OF CHINA TECH THREAT

Roslyn Layton, PhD
Founder, China Tech Threat

October 18, 2021

Table of Contents

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program	)	ET Docket No. 21-232
	)	
Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program	)	EA Docket No. 21-233

CHINA TECH THREAT'S REPLY TO COMMENTS

I. INTRODUCTION AND SUMMARY

China Tech Threat (CTT) respectfully submits this Reply to Comments regarding the Commission's *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program* and *Competitive Bidding Program* proceedings, Docket Nos. 21-232 and 21-233. CTT will address certain comments in the record and wishes to make the following points: (1) Selling electronic equipment is a privilege, not a right. (2) The proposed regulation will open a level playing field for lawful equipment providers. (3) Provided that the FCC expands Covered List entities to reflect the reality of unacceptable national security risk, only Covered List entities should be subjected to additional obligations. (4) The regulation should focus on future prohibitions, not revocation of past authorizations. (5) The proposed regulations reflect a clear, distinct mandate from Congress to the FCC to act; the regulations close a loophole created by National Defense Authorization Act (NDAA) and Entity List designations; and therefore do not duplicate or disrupt other federal cybersecurity obligations.

II. COMMENTS

1. Selling electronic equipment in the US is a privilege, not a right.

Some petitioners have opposed elements of the NPRM on grounds that the proposed regulations would disrupt enterprise. It is true that prohibiting future authorizations for Covered List entities would disrupt some revenue for some providers. However, equipment authorization is a privilege, not a right, for entities which uphold the laws of the US. The opening paragraph of the Communications Act of 1934 notes its 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 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.

Presently US law and 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 FCC rules allow vulnerable equipment to be marketed and installed into countless locations across the US. This puts millions of Americans at risk for intrusion by actors from the government of the People's Republic of China (PRC) and endangers Americans' security, privacy, and property. Given the facts and determinations by the 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.

2. The proposed regulation will open a playing field for lawful equipment providers.

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 strengthens and improves the playing field for

lawful providers with acceptable risk. The presence of vulnerable PRC-owned actors in the market creates market barriers and distortions. As observed in comments from the Coalition for Prosperous America,

> "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."[1]

Among the goals of the FCC's equipment authorization program is to promote competition through efficient, transparent, and rule-based system. However, the FCC could undermine its own program by approving entities which do not uphold the laws and values of the US. Without FCC intervention, certain categories of electronic equipment could become monopolized by PRC vendors. This has been observed with certain kinds of communications equipment, solar panels, flat panel displays, and light emitting diodes (LED), among other products.

One of the key benefits of US federal policy to restrict ZTE and Huawei is that it has allowed South Korea's Samsung to get a foothold in the US market. Samsung and other non-PRC providers likely struggled in the face of ZTE's and Huawei's aggressive and predatory practices. Indeed the US market is for network equipment is growing, despite the restrictions on

[1] Coalition for a Prosperous America. Comments filed to the FCC in 21-232 and 21-233. September 20, 2021. https://www.fcc.gov/ecfs/filing/10920200267327

Chinese military providers.[2] It is the job of the regulator to restrict a player which disobeys the rules so that the legitimate game can continue.

Presently there are still significant international competitors in the US electronic equipment market even if the Covered List entities are removed. Petitioner IPVM noted that "there are at least 40 manufacturers (not brands or relabellers but companies that develop their own video surveillance products) that would fill the gap including from the USA as well as allies including South Korea, Taiwan and the EU."[3]

3. **Provided the Covered List is updated to reflect the reality of the many equipment providers which pose unacceptable national security risk, only Covered List entities should be subjected to additional obligations.**

Some petitioners have opposed the NPRM on grounds that the proposed regulation would create needless cost and burden. The Consumer Technology Association (CTA), for example, commented that the NPRM "would burden 'good actor' companies with no guarantee of a national security benefit" and "would disrupt the smooth functioning" of the Commission's existing authorization process.

First, the FCC should not be afraid to examine, update, and refine its equipment authorization process to ensure that it comports with the law and does not present unacceptable national security risk. The notion that the FCC would refuse to address recognized security concerns because it upsets a company's revenue stream is not justified. It is not the job of the

[2] Matt Katko. Ericsson, Cisco, Samsung Gain Telco Gear Share as Huawei, Nokia Suffer Losses. SDXCentral. Sept 13, 2021. https://www.sdxcentral.com/articles/news/ericsson-cisco-samsung-gain-telco-gear-share-as-huawei-nokia-suffer-losses/2021/09/

[3] "40+ Alternatives to Dahua & Hikvision For Video Surveillance Camera Manufacturing," 17 Aug 2021. https://ipvm.com/reports/hikvision-dahua-alternatives-directory", https://ipvm.com/reports/hikvision-dahua-alternatives-directory?code=FCC

FCC to maximize revenue for firms.

China Tech Threat recognizes the point of view of CTA, a leading trade association with 1,400 members. In part because of China's dominance of the global supply chain for electronics, the profit margins of many electronics providers are slim to none. Naturally any such company is loath to accept new regulation that could add cost and reduce profitability.

However, China Tech Threat believes that the entities of concern can be identified through the process established by the 2019 Secure and Trusted Network Act and subsequently restricted without disrupting the larger industry. China Tech Threat does not think that increased obligations need to be applied to the entire industry, only to those entities which are added to the Covered List. As such, the legitimate playing field for lawful equipment providers should be preserved, if not strengthened.

It could be the case that many US equipment providers have relationships with Covered List entities, whether existing or prospective entities. China Tech Threat believes that these relationships are not in the public interest as they provide the Covered entity an undeserved benefit and the appearance of trust and credibility because of an association with a US firm. This is distortionary to American consumers.

That US firms could lose revenue from ending such partnerships should not be a concern of the FCC. If these US firms had their customers' safety and security in mind, they would not pursue relationships with PRC government-owned firms in the first place. Indeed, the FCC should not reward such irresponsible behavior with grants to reimburse and replace equipment and losses. The information about the risks and threats of IT providers owned and operated by the Chinese government has been in the public domain since at least 2005 when the United

States-China Economic and Security Review Commission (USCC) described the dangers of Huawei to Congress,[4] and again in 2009 in a report titled "China's Information Technology Giants: Huawei and Lenovo" demonstrating how Lenovo is the same as Huawei for its strategy of techno-nationalism and the associated risk for PRC intrusion.[5]

CTT 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 enables and multiplies the risk of equipment with unacceptable national security risks. The current process is not sufficiently rigorous to weed out risky suppliers and equipment.

As China Tech Threat observed on the question of technological risk in comments it filed with BluePath Labs, a leading consultancy to the US military and national security agencies, the number of potential entities which should be added to the Covered List is significant. The filing described China's Military Civil Fusion Strategy (MCFS) and China's own estimation of some 900 information technology firms which participate in the effort, many of these which operate in the US. By way of example, the comments described how following the 2019 Secure and Trusted Network Act process would add Lenovo and Yangtze Memory Technology Inc. (YMTC) to the Covered List. Similar analysis by petitioner Jordan Brunner described how SZ DJI Technology Co (DJI), Lenovo, and TikTok should be added to the Covered List.

As such, for the FCC's Covered List to be accurate, it must reflect the reality of the many

[4] USCC Annual Report to Congress, 2005. https://www.uscc.gov/sites/default/files/annual_reports/2005-Report-to-Congress.pdf
[5] USCC Annual Report to Congress, 2009. https://www.uscc.gov/sites/default/files/annual_reports/2009-Report-to-Congress.pdf

firms that apply for equipment authorizations and pose an unacceptable national security risk. As such, the FCC's Covered List should be expanded to add the firms which fulfill the requirements defined by the 2019 Secure and Trusted Networks Act.

4. The regulations should focus on future prohibitions, not revocation of past authorizations.

China Tech Threat applauds the FCC for contemplating the revocation of authorizations granted to Covered Entities. The FCC observes at least 3,000 authorizations have been granted to Huawei alone since 2018. This is a staggering figure, and the FCC is correct that the equipment associated with these authorizations poses an unacceptable risk. Indeed, the FCC has developed an elaborate (and in China Tech Threat's view, overgenerous) reimbursement program for Universal Service Fund providers. In China Tech Threat's view, providers that prioritize the safety of their customers do not use equipment produced by Chinese military and government entities.

However, China Tech Threat is sensitive to the concerns of various petitioners who note the confusion that revocation could create for the industry at large. Several petitioners raised concerns that revoking existing equipment authorizations could unduly burden manufacturers acting in good faith and disrupt US supply chains. CTIA noted that revoking existing authorizations could have "unintended consequences… across the entire ICT economy."

Given that the regulation represents an important change to the FCC's equipment authorization process, China Tech Threat believes it is reasonable for the FCC to prohibit future authorizations while leaving past authorizations in place. This can allow the FCC time 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.

5. The proposed regulations reflect a clear, distinct mandate from Congress to the FCC and therefore do not duplicate or disrupt other federal cybersecurity obligations.

China Tech Threat applauds the FCC for conducting this proceeding with faithful attention to process, rule of law, and Congressional oversight. CTT finds that the FCC has built the record for these actions in a consistent, dedicated manner over years. Its actions are reasoned and justified.

Some petitions claim that the FCC's proposed rules could duplicate, if not disrupt, other federal cybersecurity obligations. 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. For the reason alone, the FCC's action is justified.

More largely, while policy instruments like the NDAA and Entity List designations are powerful instruments, they create major loopholes. For example, the NDAA only restricts federal procurement. This leaves states, businesses, and individuals to purchase what they want, which unwittingly is unrestricted, vulnerable equipment. The Entity List imposes a license requirement on firms wishing to transact with the entity of concern for certain kinds of products. This does not address the security risks created by use of hundreds, if not, thousands of IT providers which do not necessarily fall on the Entity List.

The proposed regulation reflects a clear, distinct mandate from Congress to the FCC to act; it closes a loophole created by the NDAA and Entity List designations; and therefore do not duplicate or disrupt other federal cybersecurity obligations. While it is understandable that CTIA wants a "unified framework" for cybersecurity at the national level, this is job of Congress, not the FCC. In fact, the FCC is doing exactly what Congress instructs it to do based upon its authority from the 1934 Communications Act.

III. CONCLUSION

With this proceeding, the FCC has made important and welcome progress to address major security risks in electronic equipment. China Tech Threat applauds the Commission for its bipartisanship and its fidelity to Congress' mandate.

Respectfully submitted,

Roslyn Layton, PhD
Founder, China Tech Threat

October 18, 2021