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

COMMENTS OF Coalition for a Prosperous America

I. INTRODUCTION

The Federal Communications Commission (FCC) undertakes this important proceeding to improve equipment security on equipment which uses radio frequency and to less the risk of intrusion from foreign and malicious entities. The Coalition for a Prosperous America (CPA) is a bipartisan coalition of U.S. manufacturers, agricultural producers and workers committed to rebuilding U.S. manufacturing and family farming and restoring broadly-based U.S. prosperity. CPA member companies create U.S. jobs, support their local communities, provide important innovation, and uphold American laws and values. As the Chief Economist, I lead a team that studies international trade, issues of economic and national security importance, inequality, and related issues. Personally, I was a technology executive working in Silicon Valley from 1997 to 2016. I competed directly with Huawei between 1998 and 2011 while employed at two leading North American networking equipment makers, Nortel Networks and Infinera. Since joining CPA in 2016, I have studied the impact of Huawei on the global market. CPA supports this proceeding. We find that restricting equipment from Covered List entities would serve the public

interest and have a positive impact on the economy and American jobs. Following are our comments for the record.

II. Restricting equipment from Covered List entities serves the public interest by improving security and increasing competition in the electronic equipment/connected device market.

CPA supports the FCC's efforts to restrict entities of the FCC's Covered List, both in revoking existing equipment authorizations and prohibiting new ones.

A. Restricting Equipment from Huawei and Covered List entities will make the U.S. more secure.

i. Huawei was founded by the Chinese military. Huawei and ZTE have a long record of being involved in espionage operations for the Chinese government, and of failing to resolve security flaws in its equipment, including network access equipment in various nations. These flaws enable espionage operations by the network equipment provider and the government of the People's Republic of China (PRC). Huawei installs backdoors in its equipment and indeed all networking equipment offers great opportunities for espionage via what is known as the "control channel," by which equipment managers communicate with and manage remote equipment. Americans who use Huawei devices are at risk for PRC surveillance, espionage, and other forms of compromised integrity.

ii. Huawei is known and well-documented to have been the perpetrator in many intellectual property (IP) theft cases. For example, in 2003 it settled a case brought by Cisco Systems that involved stealing IP for Cisco routing

technology that was worth billions of dollars. Its early start in the networking business is largely attributed to multi-billion dollar subsidies by the PRC government and copying and/or stealing western technology from its competitors.

B. Restricting Equipment from Huawei and Covered List entities will improve competition in the market for connected devices.

i. 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.

C. Restricting Equipment from Huawei and Covered List entities coupled with incentives for U.S. manufacturing can restore American jobs and improve equipment security by removing the PRC from the supply chain.

i. The FCC rightly recognizes that it is not enough to restrict vulnerable equipment and vendors; there should also be incentives to improve security. CPA believes that an important part of this security comes from U.S.-based ownership and production.

ii. The U.S. technology food chain has a growing number of gaps and holes that endanger U.S. national security and represent lost economic opportunity. By food chain, we mean everything from small electronic components through

semiconductors (integrated circuits) to subsystems and complete networking and computer systems.

iii. 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. The choice between heavily subsidized Chinese vendors and undercapitalized European vendors favors increased growth and market dominance by Chinese vendors unless the U.S. takes decisive action.

iv. The semiconductor, also known as an integrated circuit or "chip" or "microchip," is the heart of modern technology. Chips were invented in the U.S. and the U.S. once accounted for more than half of global chip manufacturing, but this has fallen to just 12 percent according to a recent Boston Consulting Group study. Not only has this resulted in the loss of high-paying jobs, but it has also intensified the problem of security by making the semiconductor itself vulnerable. The importance of chips in modern products is growing. For example, experts estimate that chips could soon account for up to 20 percent of the value in a car. We could soon have 100 million cars on U.S. roads, all run by semiconductors and communicating with each other and a central network via wireless connections. Yet we are in danger of losing the ability to manufacture these essential semiconductors. Current severe shortages provide a preview of the seriousness of the problem.

v. Further, the growing ubiquity of semiconductors in technology devices, vehicles, household appliances, and shipping tickets on every package moving

around the U.S. increase the opportunities for espionage and exploitation of chip vulnerabilities by the PRC or other hostile powers.

vi. For more background, see the attached CPA white paper on *MAINTAINING U.S. LEADERSHIP IN SEMICONDUCTORS AND COUNTERING CHINA'S THREATS*, also available online at https://prosperousamerica.org/cpa_china_tech_threat_release_white_paper_on_semiconductors_countering_china_s_threats/ which provides background on American manufacturing and the security threats from China, including the compromise of integral components like semiconductors.

III. CONCLUSION

Thank you for conducting this proceeding. I am happy to provide further information.

Respectfully submitted,

Jeffrey Ferry
Chief Economist
Coalition for a Prosperous America

Dated Sept. 16, 2021