EXHIBIT G

Declaration of Bryant Tow on FCC-18-42A1: Notice of Proposed Rulemaking: Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs: WC Docket 18-89

1. My name is Bryant Tow. I am over 18 years of age and competent to testify.
2. For over 25 years I have held responsibilities as an entrepreneur and senior executive in all aspects of risk management including thought leadership in the area of cyber security, award winning development of security solutions, managing large global cyber and physical security teams. I have served on the DHS Sector Coordinating Council, ISSA, ISACA and InfraGard National Members Alliance board member and VP. I have been recognized as a Distinguished Fellow by the Ponemon Institute and have published several books and articles on cyber security topics and has received several awards for my contributions to the industry.
3. Citing National Security, the Federal Communications Commission (the Commission or FCC), at its open meeting on April 17, 2018, adopted a Notice of Proposed Rulemaking ("NPRM" or "the Notice"), FCC-18-42A1, to consider a rule which would prohibit Universal Service Fund ("USF") support from being used to purchase or obtain any equipment or services produced or provided by a company posing a national security threat to the integrity of communications networks or the communications supply chain.
4. I have been retained as a consultant by counsel to offer my expert opinion on whether the NPRM, if adopted, would be likely to achieve its stated goal of improving national security. For the reasons outlined below, I conclude that any benefits to national security would be marginal, and likely insignificant. In particular, the NPRM focuses only on the final seller of equipment and services, and fails to address threats arising from suppliers of components incorporated into the final products, many of which originate from China. It also fails to ignore potential threats arising after the production of equipment, at subsequent stages of the supply chain. It only considers the identity of the manufacturer, not the nature of the equipment, and therefore does not differentiate based on the level of risk posed by a specific purchase. And it does not take into account the level of threat, since recipients of USF support are not the likely targets of any hypothetical cyberattack initiated by a hostile government or other actor.
5. The NPRM seeks comments on the proposed rule, including its potential scope and various implementation issues. This includes questions around how any FCC ban on the integration of equipment provided by the various companies into subsidized U.S. networks might work.
6. Additionally, there are scope questions on how to identify companies that pose a national security threat to communication networks or the communication supply chain. The

NPRM asks whether the Commission should establish the criteria for identifying a covered company, and if so, how should it be determined.

7. The FCC has no stated expertise in risk ranking any company or nation state on the level of national security risks. The FCC would have to rely upon another federal agency to maintain the list of communications equipment or service providers that raise national security concerns regarding the integrity of communications networks or the communication supply chain.

8. Given the Commission's lack of familiarity with supply chain control and issue awareness, it is perhaps not surprising that the Notice focuses on interdicting named companies rather than focusing on the complexity of addressing supply chain risks, such as the fact that components made by multiple companies in multiple countries are usually embedded within the products of other entities.

9. It is clear that the NPRM has relied on the previously voiced concerns of US intelligence agencies and lawmakers that specific companies such as Huawei and ZTE could help countries such as China compromise the security of networks in the United States. Although these claims have, so far, been based on no public evidence, the NPRM implies that both Huawei and ZTE would likely be blacklisted entities. Although years of espionage fears have left both companies with a minuscule presence in the current domestic market, this appears to be nothing more that the FCC trying to weed them out entirely as carriers march toward 5G and the next generation of wireless networks. It should be noted no substantial proof of espionage by China or Huawei has ever been established from these accusations and the House intelligence committee report released at the time did not offer much in terms of substance either.[1]

National security implications of imported technology incomplete

10. The Rule, while well intended, misses several other more likely attack vectors and ignores the complexity of the supply chain. For example, memory, chipsets and semiconductors products from several manufacturers are included in nearly every consumer, corporate, critical infrastructure and even military device. There are a multitude of products which have been operating under already high security "Orange" and "Red Book" compliance requirements for a number of years without national security implications. Many of these manufacturers operate in Taiwan and produce components in China. A few examples:

    a. ***Apacer*** is headquartered in Taiwan and has offices in Shanghai, Peoples Republic of China. It manufactures cloud computing servers, transportation processors, embedded and IPC, defense, gaming and healthcare components used throughout the US. Their chips state compliance with MIL-STD-810G(SSD) &MIL-STD-

[1] https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

202G(DRAM) as well as MIL erase standards including DoD 5220.22-M, NSA Manual 130-2, USA AF AFFSSI 5020, USA Army 380-19, USA Navy NAVSO P-5239-26IREC(IRIG) 106 and NSA 9-1. Additionally, they produce Car Area Network "CAN" Bus Cards that control a vehicles central nervous system.

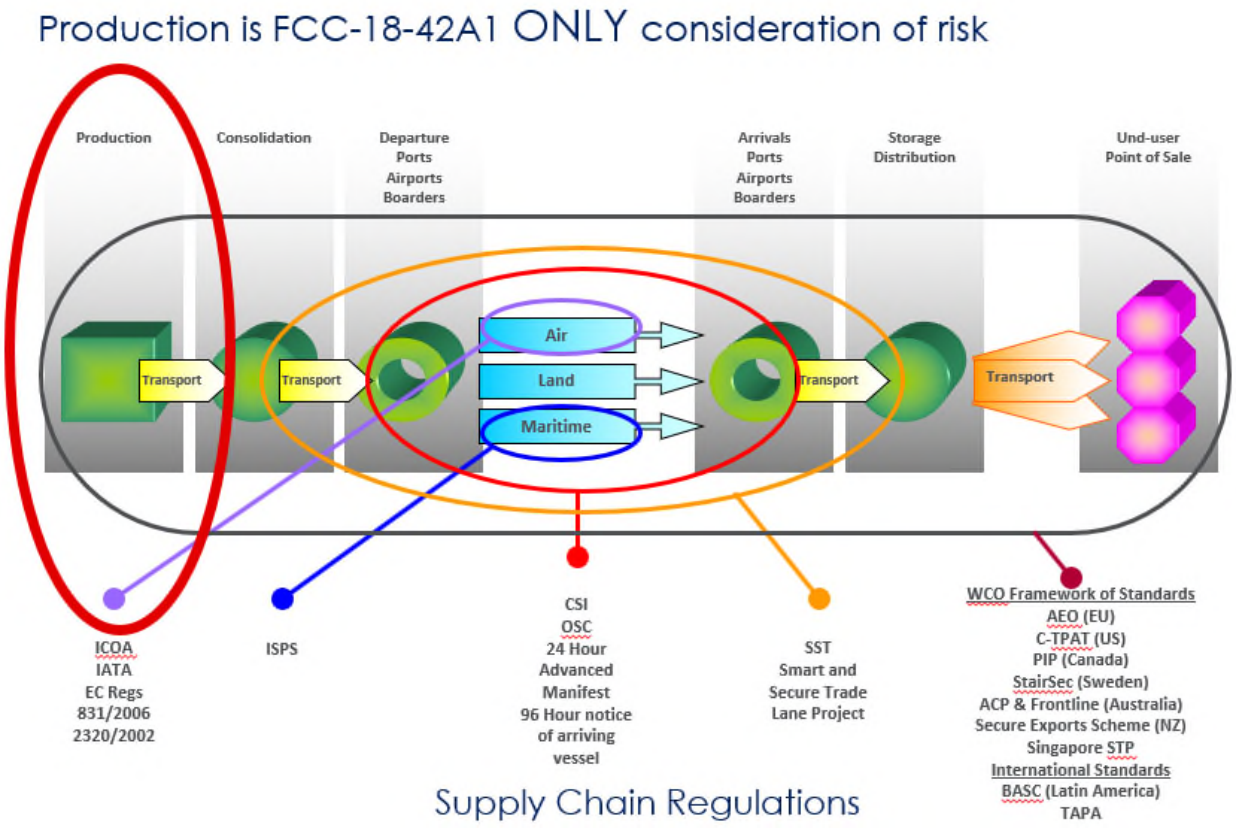
b. ***Asus*** is a Taiwanese multinational computer and phone hardware and electronics company headquartered in Beitou District, Taipei, Taiwan. Its products include desktops, laptops, netbooks, mobile phones, networking equipment, monitors, WIFI routers, projectors, motherboards, graphics cards, optical storage, multimedia products, peripherals, wearables, servers, workstations, and tablet PCs. The company is also an original equipment manufacturer (OEM). One of their manufacturing facilities is located in Suzhou, Chongqing, PRC.

11. Additionally, it should be noted the attack vectors extend well beyond a few routers, switches and phones. Chinese firms are not only responsible for final assembly and shipping products abroad, they also form a large portion of the overall supply chain of manufacturing electronic components used in nearly every electronic device manufactured globally. That includes not just smartphones and mobile devices, but also the Internet of Things (IoT), major appliances, medical devices, automobiles, aerospace, etc. Infiltration through these goods could reach much higher value targets with more precision and broader reach than merely the devices purchased through the USF. Yet the FCC's proposal does not consider any of this in proposing to single out Huawei and ZTE, apparently for no other reason than their Chinese origin.

Logistical and supply chain risks not considered

12. Banning products only based on the source country of the final manufacturer does not consider other logistics and supply chain risks. In the FCC's proposed rule as written, only final production is considered. Potential threats could be introduced at: consolidation, border crossings, storage & distribution and last mile transport. As illustrated below, multiple organizations across the globe have numerous regulation methods and standards for identifying, assessing, measuring and managing potential threats to the logistics movement of goods across the supply chain including air, land and maritime

transportation. Yet the FCC in its proposed Rule has only chosen to address a portion of the production phase of the supply chain.



Impact on national security by USF supported organizations

13. Even if the FCC proposal did materially reduce supply chain vulnerabilities (and it does not), its effectiveness in protecting national security would be debatable at best. Most recipients of USF support are small, rural carriers; school districts; public libraries; and rural health care providers. These are not the high-value targets that a foreign government or its agents would be likely to target with a cyberattack or disruption of supply. While there has been no published evidence of back doors or other compromises, if one should be discovered at a USF supported organization, "National Security" does not immediately come to mind as a potential risk.

Broad nature of risk ranking by 'Company'

14. The rule as stated would prohibit any USF funds from being used to purchase 'any' product from a company listed as a national security risk. Associating the level of risk at the company level does not consider the implication of the product(s) for potential purchase. Some products from these companies could potentially be of a nature that could not possibly pose a technology or other national threat. But the FCC makes no effort to evaluate or distinguish among potential risks based on the nature of the products purchased.

Past U.S. measures against Chinese based suppliers have had a negative impact on overall competition in the U.S. Telecom Equipment Market

15. The U.S. telecom equipment market is worth $30 billion a year. As the U.S. government has previously taken various measures to block Huawei and ZTE, the U.S. market is now dominated by two Nordic telecoms giants, Ericsson and Nokia, in contrast to the global market where Huawei and ZTE both have a strong presence.

16. According to market research firm Dell'oro, less than one percent of mobile and fixed-line devices in the U.S. now comes from Huawei. The FCC decision means that Huawei will likely lose even their small share of the U.S. telecom equipment market.

17. Huawei has continuously been met with obstacles since it entered the U.S. market a decade ago. These past actions have had a significant negative impact of the overall competition in the U.S. telecommunication market. The additional measures imposed by the NPRM will increase risk and place further stress on the U.S. market, likely leading to fewer choices, higher prices, the risk of future market shortages and the potential loss of the U.S. advantage around future technology advances.

Conclusion

18. The NPRM includes new punitive measures that appear to be designed to weed Chinese companies entirely out of the US market as carriers march toward 5G and the next generation of wireless networks.

19. As the NPRM is currently written, there are concerns around the accuracy with which national security threats are identified, around definitions and the scope of its application, what equipment and services would be covered and the feasibility of its implementation. Accordingly, the Commission appears to have had to resort to focusing on interdicting named companies versus performing a more reasonable threat

assessment and evaluation to determine the real threats and vulnerabilities in order to reduce risk.

20. Accordingly, the potential benefits of the proposed rule, in terms of reducing risk to the national security, will be marginal at best, and therefore insignificant.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on May 31, 2018.

Bryant Tow