Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs	)	WC Docket No. 18-89

REPLY COMMENTS OF HYTERA COMMUNICATIONS CORPORATION LIMITED

Hytera Communications Corporation Limited ("Hytera"), by its counsel, hereby submits Reply Comments regarding the Commission's recent Public Notice in this proceeding.[1] The Notice requests comment on the applicability of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (the "NDAA") to the Commission's *Protecting Against National Security Threats to the Communications Supply Chain* rulemaking.[2]

Introduction

Hytera is a privately held corporation organized under the laws of China, and listed on the Shenzhen Stock Exchange. Hytera, and its subsidiaries, manufacture and supply land mobile radios ("LMR") systems and solutions to customers in 120 countries throughout the world including the United States, in a range of sectors including government, public utilities, transportation, hospitality, and education.

---

[1] Public Notice, *Wireline Competition Bureau Seeks Comment on Section 889 of John S. McCain National Defense Authorization Act for Fiscal Year 2019,* WC Docket No. 18-89, DA 18-1099 (released October 26, 2018)("Public Notice").

[2] Notice of Proposed Rulemaking, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* WC Docket No. 18-89, FCC 18-42, 33 FCC Rcd 4058 (2018)("NPRM").

In May of 2018, Hytera's name was added to Section 889 of the House of Representatives version of NDAA, without notice to Hytera and without affording Hytera the opportunity to respond to any national security concerns that Members of the House may have had. In August 2018, the NDAA was signed into law by President Trump, including Section 889 which identifies Hytera.[3]

Discussion

The Commission identifies as it four "Strategic Goals":[4]

1. Promoting Economic Growth and National Leadership
2. Protecting Public Interest Goals
3. Making Networks Work for Everyone
4. Promoting Operational Excellence

For the first three goals, the Commission identifies promoting and maintaining competitive telecommunications networks as a vital component in achieving the strategic goals.[5] *Id.* Engaging in the rulemaking process to implement the NDAA without careful and deliberate coordination between federal agencies, and importantly without affording affected entities due process, and without fully engaging the stakeholders, is contrary to the Commission's strategic goals.

The NDAA, by its very terms, implicates subject matter outside the expertise of the Commission, and thus, implementation of the NDAA requires, at a minimum, the expertise of

---

[3] Public Notice, pp 1-2.

[4] https://www.fcc.gov/about/overview accessed on December 4, 2018.

[5] *Id.*

the following U.S Federal Agencies: the Department of Defense (DOD), the General Services Administration (GSA), the National Aeronautics and Space Administration (NASA) and the Department of Homeland Security (DHS). By happenstance, the Commission issued the present NPRM months before the NDAA was enacted. In view of the subsequent enactment of the NDAA and its potential impact on the Commission's vital component of promoting and maintaining competitive telecommunications networks, and for the reasons stated below, the Commission should take this opportunity to pause the present proceeding to afford time to engage with other federal agencies with national security jurisdiction. This will enable the Commission to ensure the rulemaking process is undertaken in a coordinated, consistent, and fair manner across the federal government.

Hytera would like to emphasize the remarkable and unfortunate position that it finds itself in. It has always implemented the highest level of cybersecurity protections for its equipment, and has never been informed by any U.S. government entity that its equipment posed a national security risk. Yet, without the most basic protections afforded by due process, Hytera was designated by name in a statute that identifies activities for which Federal agencies are prohibited in engaging with Hytera. Hytera understands and supports the efforts by Congress to protect U.S. telecommunications infrastructure from cybersecurity risks, and will work alongside all U.S. government entities to achieve this mission. The Commission must ensure its proceedings are not improperly utilized for anti-competitive tactics which deprive telecommunications vendors of due process, unfairly discriminate against providers, and improperly restrict competition.

The Commission should be careful not to read Section 889 too broadly. The NDAA's language is only intended to deal with federal procurement -- not procurement of identified

equipment with private funds: "Congress drafted Section 889 as a ban on federal procurement, not commercial possession."[6] Future Commission rules should make this distinction conspicuous and clear to end-users of equipment.

Beyond this, it is evident that a coordinated, consistent approach toward perceived telecommunications cybersecurity concerns, is in order. As NCTA observes, "a cohesive, whole-of-government application will be critical to ensure that the security concerns animating enactment of that section are addressed in a consistent and uniform manner across the Federal government."[7] This is especially the case when it comes to the NDAA, and cybersecurity risks.[8]

The Commission should coordinate with federal agencies with expertise in assessing cybersecurity risks. In the case of the NDAA, DOD is the lead agency, along with DHS also having a primary role. DHS has recently stood up a new agency, the Cybersecurity and Infrastructure Security Agency within the Department.[9] In addition, DHS has established the National Risk Management Center whose function is to help foster government-industry cooperation on cybersecurity risk reduction.[10] The DHS ICT [Information and Communications Technology] Supply Chain Risk Management Task Force is also working on recommendations in this area.[11]

---

[6] Comments of Telecommunications Industry Association, WC Docket No. 18-89, at 24 (November 16, 2018)("TIA Comments").

[7] NCTA – The Internet and Television Association letter, WC Docket No. 18-89 at 3 (November 16, 2018). See also USTelecom Association ex parte letter, WC Docket No. 18-89 (September 20, 2018).

[8] Comments of ITTA – The Voice of America's Broadband Providers, WC Docket No. 18-89 at 2 (November 16, 2018)("other governmental entities are better poised to address foreign cybersecurity threats than the Commission").

[9] https://www.dhs.gov/CISA accessed on December 4, 2018.

[10] https://www.dhs.gov/cisa/national-risk-management-center accessed on December 4, 2018.

[11] https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology accessed on December 4, 2018.

The focus for implementation of the NDAA, and ultimately any determination by the Commission as to its own responsibilities, should not be on supply chain management.[12] Rather, consistent with the need to "to develop a clearer, focused policy that addresses real harms,"[13] the focus should be on specific suppliers and, more importantly, specific equipment of those suppliers, and should include robust due process protections. In this regard, the NPRM suggests that the Commission might even direct its focus to the component level.[14] Certainly, any approach which blacklists all manufacturers from a specific country or countries, or all of the equipment from those entities, would be a disservice to American consumers who would be deprived of the opportunity to choose equipment that is otherwise safe, secure and competitive. Moreover, "an overbroad rule or blanket country-of-origin ban could harm U.S. international trade interests without effectively improving security."[15]

DOD, GSA and NASA have initiated a proceeding that looks toward developing consistent guidance for the implementation of the NDAA.[16] That proceeding would be one possible vehicle for resolving the numerous ambiguities in Section 889. DHS and its instrumentalities represent another important avenue. It must be stressed that the NDAA is not self-executing; i.e. numerous issues must be resolved, "including which suppliers are prohibited,

---

[12] Telecommunications Industry Association ex parte filing, WC Docket No. 18-89 at 3 (October 1, 2018).

[13] Computer & Communications Industry Association Comments, WC Docket No. 18-89 at 4 (November 16, 2018).

[14] NPRM at para. 15 (referencing "which components or services are most prone to supply chain vulnerabilities?").

[15] TIA Comments at 17. TIA also suggests that "an appropriate strategy would be to focus on particular suppliers and even on particular products within their portfolios – *i.e.*, using a scalpel rather than a hatchet." Comments of the Telecommunications Industry Association, WC Docket No. 18-89 at 46 (June 1, 2018).

[16] *Federal Acquisition Regulation Case 2018-017, Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment*, 83 Federal Register 58110 (Nov. 16, 2018).

which types of equipment and components are covered, and how compliance with the prohibition should be certified and/or verified."[17]

Take, for example, the meaning of the term "telecommunications equipment" which appears in several sections of the NDAA, but is undefined. However, "telecommunications equipment" is defined in the Communications Act; namely, as "equipment, other than customer premises equipment, used by a carrier to provide telecommunications services, and includes software integral to such equipment (including upgrades)." 47 U.S. Code Section 153(52). In other words, absent connection to a carrier's network, there is no "telecommunications equipment." In the communications field, use of the term "telecommunications equipment" excludes, for example, equipment which is not connected to a carrier's network like private mobile radio systems licensed under Part 90 of the Commission's Rules for internal business communications.[18] Presumably, the Communications Act definition as implemented by the Commission -- being the expert agency in communications matters -- was the one intended. However, the Commission's failure to take an active role engaging other agencies may result in inconsistent definitions being used across federal agencies and unintended consequences that inhibit rather than promote competitive telecommunications networks. The NDAA includes other language, some of which implicates the expertise of the Commission, and this language too

[17] TIA Comments at 16.

[18] See 47 U.S. Code Section 332(d) defining "private mobile service," in pertinent part, as "any mobile service (as defined in section 153 of this title) that is not a commercial mobile service or the functional equivalent of a commercial mobile service;" "commercial mobile service" as "any mobile service . . . provided for profit and makes interconnected service available (A) to the public or (B) to such classes of eligible users as to be effectively available to a substantial portion of the public; and "interconnected service" as "service that is interconnected with the public switched network (as such terms are defined by regulation by the Commission . . . ." (emphasis added).

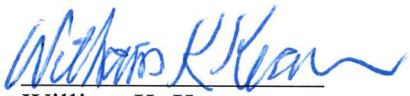
must be clarified such that a uniform approach across the government is achieved.[19]

Finally, provisions must be made for affected entities to appeal an adverse determination on the cybersecurity risk of their equipment as this is a matter of fundamental fairness and due process.

CONCLUSION

Hytera does not take issue with the intent which has motivated the NDAA. However, in implementing the law, the Commission and other agencies should be careful not to sweep overly broadly, lest innocent vendors, and equipment posing no cybersecurity risk, be barred. Such a result would be to the detriment of American consumers and could inadvertently feed overtly protectionist actions by other administrations masquerading as cybersecurity protection.

Respectfully submitted,



William K. Keane
Patrick McPherson

DUANE MORRIS LLP
505 9th St NW, Suite 1000
Washington, DC 20004
202-776-5243

Counsel for Hytera

December 7, 2018

[19] The references to "public safety, security of government facilities, physical security of critical infrastructure, and other national security purposes" in Section 889(f)(3)(B) and "substantial or essential component" and "critical technology" in Section 889(a)(1), are to like effect, as are terms such as the exemption for equipment which "cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles" in Section (b)(3)(B). None of these terms are defined. Issues like these are best addressed with advice and consultation from DHS, DOD, and other agencies.