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

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

WRITTEN *EX PARTE* SUBMISSION OF HUAWEI TECHNOLOGIES CO., LTD AND HUAWEI TECHNOLOGIES USA, INC.

Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"), by their undersigned counsel, submit this *ex parte* presentation to supplement the record in the above-captioned docket.

Recent events require that Huawei supplement the extensive evidence already in this docket that banning particular vendors on grounds of "national security" will actually do little or nothing to protect the security of America's telecommunications networks. Rather, forcing network operators to rip out and replace their existing equipment would pose a greater threat to network stability and security. In addition, recent public comments of a top Executive Branch official confirm that concerns about supposed "backdoors" in Huawei's telecommunications equipment are *not* at the root of recent Government actions against the company. Comments by other officials from the United States and elsewhere cast further doubt on the wisdom of taking a company- and country-agnostic approach to 5G wireless network security. Not only would a policy of targeting specific vendors be insufficient to address supply chain concerns, it may also cause the United States to violate its international trade obligations.

Huawei cannot and will not sabotage its customer networks. But recent actions by the United States Government are only one step away from doing so. In early April, Chairman Pai

said the FCC is quickly trying to wrap up the above-captioned rulemaking, and the FCC was working with the National Telecommunications and Information Administration of the Department of Commerce in connection with the rulemaking.[1] On May 16, the Department of Commerce added Huawei to its Entity List,[2] thereby restricting exportation of U.S. products and technologies covered by the Export Administration Regulations to Huawei and 68 of its subsidiaries, citing a January indictment and national security as grounds for the decision. Although Huawei Technologies USA, Inc. was not added to the Entity List, and importation of Huawei equipment from China is not affected by this action, the ban would impair Huawei Technologies USA and its customers' ability to have technical exchanges with Huawei Technologies Co., Ltd. On the same day, President Trump signed an executive order that allows the Commerce Department to ban or regulate foreign telecommunications equipment that poses a national security risk to the technology infrastructure of the U.S..[3] Also on the same day, Commerce Secretary Wilbur Ross said in an interview that "[m]any of the rural telecom carriers are already using Huawei in the 4G environment and in order not to have them have to rip everything out, we'll be dealing with that separately."[4] On the following Monday, the Department of Commerce issued a 90-day Temporary General License

---

[1] Multichannel News, "Pai to Hill: We Hope to Move Quickly on USF Suspect-Tech Ban", https://www.multichannel.com/news/pai-to-hill-we-hope-to-move-quickly-on-usf-suspect-tech-ban (April 4, 2019).

[2] Bureau of Industry and Security, *Addition of Entities to the Entity List*, 84 Fed.Reg. 22961 (May 21, 2019).

[3] Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 Fed.Reg. 22689 (May 17, 2019).

[4] Wilbur Ross on Huawei: Many Rural Telecom Carriers Already Using it in 4G Environment (May 16, 2019), *available at:* https://video.foxbusiness.com/v/6037617623001/#sp=show-clips.

authorizing transactions with Huawei necessary to continued operations of existing networks and equipment, among several other types of transactions.[5]

Given the imminent adverse impact to Huawei and its U.S. customers' business, Huawei has been trying to schedule ex parte meetings with all of the Commissioners to learn first-hand and directly address their concerns over the company. However, no Commissioner has yet agreed to meet personally with Huawei.[6] While Huawei has not been provided with the basis or any supporting evidence for the government's adverse actions and is therefore handicapped to respond, one thing is clear – the USF rulemaking would significantly impair the operations of many rural carriers and put those carriers' end user customers at risk of service interruptions, even if the Commerce Department does not demand removal of Huawei equipment. No evidence shows Huawei has the ability or intent to shut down its customer networks, yet this rulemaking threatens to do exactly that. In a recent interview, Nemont Telephone Cooperative CEO Mike Kilgore challenged the Commission's rulemaking, saying, "Nobody in their right mind would shut down a network and shut down public safety." Subscribers from the same northeastern Montana region explained how Huawei networks keep the community safe in the event of problems and fires, as well as up-to-date with latest planting data and vital weather reports, and that even a temporary shutdown of the network would cause safety risks.[7] In short, the Commission's proposal to bar use of equipment from particular targeted vendors would cause extensive harm without solving any real problem.

---

[5] Bureau of Industry and Security, *Temporary General License*, 84 Fed.Reg. 23468 (May 22, 2019).

[6] Several Commissioners offered to have their aides meet with Huawei representatives, but several other offices did not respond at all to Huawei's meeting requests.

[7] CGTN America, "Huawei ban may impact rural US Midwest mobile operators", https://www.youtube.com/watch?v=qzazkQPM8eI (May 27, 2019).

Further, if, as Secretary Ross has suggested, the Government develops measures that will allow carriers with existing Huawei equipment to continue using it at some (so far) unknown additional cost without undue risk to national security, it logically follows that the same measures should mitigate any risk to national security posed by future installation of similar equipment by any other carrier. It would be irrational to permit the use of embedded equipment yet prohibit new purchases of the same equipment, subject to the same protective measures.

Indeed, even members of the Administration have conceded that targeting specific vendors is neither necessary nor sufficient to ensure network security. Susan Gordon, Principal Deputy Director of National Intelligence, spoke at a recent symposium held at the University of Texas at Austin titled "Intelligence in Transition." In response to a question regarding whether intelligence sharing through the Five Eyes framework is at risk if the United Kingdom permits the use of Huawei equipment, Ms. Gordon stated that concern about Huawei's inclusion in foreign countries' networks is "not an issue of technological backdoors because I can test for those."[8] Rather, Ms. Gordon indicated that the true concern is about the "compelling of the data" by the Chinese government (which, as Huawei has explained in prior filings, is not actually permissible). Instead of banning use of technologies or equipment from certain providers, Ms. Gordon explained that protecting global telecommunications networks in the 5G era will be an exercise in risk management, stating that "We are going to have to figure out a way in a 5G world that we're able to manage the risks in a diverse network that includes technology we can't trust. We're just going to have to

---

[8] *See* Susan Gordon, Principal Deputy Dir. of Nat'l Intelligence, Keynote Address at the University of Texas Austin Symposium: Intelligence in Transition (April 1, 2019), http://www.ustream.tv/recorded/120831061 (last visited May 2, 2019).

figure that out."[9] These comments about the nature of the alleged threat posed by Huawei – made in a public forum by a top intelligence official of the United States Government – lay bare the notion that concerns about Huawei equipment stem from alleged intentional insertion of technological vulnerabilities or backdoors into Huawei's products or those products produced by other Chinese companies.

While Huawei does not agree with the view that Chinese companies pose a threat simply because they are Chinese, Huawei agrees that threats to network security do exist, and should be addressed comprehensively through a holistic approach to supply chain security, not through a vendor-by-vendor approach. Similar to Ms. Gordon's apparent endorsement of a risk management response to potential threats in the 5G era, other senior Administration officials appear to support this approach, stating that the security effort of the Administration is "country and company agnostic."[10] Similarly, Huawei recalls the insightful comments of Rep. Greg Walden, then-Chairman of the Energy and Commerce Committee, during a White House 5G Summit, emphasizing that:

> It's critical we continue to focus on mitigating risks to the global supply chain of communications equipment and services. There have been alarm bells at all levels of government about potential risks to the supply chain. But some of the proposed solutions can be just as alarming.
>
> There are some who think we can simply ban vendors from American markets. But the marketplace for hardware and software is global. Without a forward-looking

---

[9] Ellen Nakashima and Souad Mekhennet, *U.S. Officials Planning for a Future in Which Huawei Has a Major Share of 5G Global Networks*, The Washington Post (April 1, 2019), https://www.washingtonpost.com/world/national-security/us-officials-planning-for-a-future-in-which-huawei-has-a-major-share-of-5g-global-networks/2019/04/01/2bb60446-523c-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.3d866f35b243.

[10] Charlie Mitchell, *Trump Officials Tout 'Holistic' and 'Country Agnostic' Effort to Secure Next-Generation Wireless*, Inside Cybersecurity (March 19, 2019), https://insidecybersecurity.com/daily-news/trump-officials-tout-holistic-and-country-agnostic-effort-secure-next-generation-wireless.

> strategy, it will be increasingly difficult for our domestic communications providers to obtain their equipment from trusted vendors.[11]

Allies of the U.S. have announced similar desires to take a holistic view of 5G network security. For example, Chancellor Angela Merkel recently explained that Germany's "approach is not to simply exclude one company or one actor, but rather we have requirements of the competitors for this 5G technology."[12] Jochen Homann, the president of Bundesnetzagentur (*i.e.*, the FCC's German counterpart), told the Financial Times that its position "is that no equipment supplier, including Huawei, should or may, be specifically excluded" and that as Bundesnetzagentur considers newly proposed security guidelines "there will be no requirements … that are aimed at a particular company."[13] Similarly, France has pursued generally applicable security and testing requirements for 5G equipment that don't single out specific companies to exclude from the market.[14] The United Kingdom's National Security Adviser also is reported to have said that the more

---

[11] Chairman Walden Delivers Remarks at White House 5G Summit, U.S. House of Representatives Energy and Commerce Committee (Oct. 1, 2018), *available at* https://republicans-energycommerce.house.gov/news/in-the-news/icymi-chairman-walden-delivers-remarks-at-white-house-5g-summit/.

[12] Paul Carrel, *Germany Not Planning to Exclude a Company from 5G Auction Per Se*, Reuters (March 19, 2019), https://www.reuters.com/article/uk-germany-politics-huawei-tech-idUKKCN1R017R. *See also* Giles Turner, *Huawei Has Skirted Outright Bans in Europe. But Not 5G Regulations*, Bloomberg (April 15, 2019), https://www.bloomberg.com/news/articles/2019-04-15/huawei-s-avoiding-outright-bans-but-not-5g-regulations-in-europe (quoting Chancellor Angela Merkel as stating: "'There are two things I don't believe in. … 'First, to discuss these very sensitive security questions publicly, and second, to exclude a company simply because it's from a certain country.'").

[13] Tobias Buck, *German Regulator Says Huawei Can Stay in 5G Race*, Financial Times (April 14, 2019), https://www.ft.com/content/a7f5eba4-5d02-11e9-9dde-7aedca0a081a.

[14] Helen Fouquet, Angelina Rascouet, and Marie Mawad, *France's 5G Bill Makes it Tough, But Not Impossible, For Huawei*, Bloomberg (April 3, 2019), https://www.bloomberg.com/news/articles/2019-04-03/france-s-5g-bill-makes-it-tough-but-not-impossible-for-huawei.

important focus is on the security of the system, not the origin of the company that made the equipment.[15] Instead of such bans, he emphasized approaching protecting their interests "through regulation, through transparency, through setting very close standards[.]"[16]

European countries are not the only U.S. allies to recognize the need for a holistic approach to managing risk in the telecommunications supply chain. Scott Jones of the Canadian Center for Cyber Security, Canada's top cybersecurity official, has said that a country-based vendor ban fails to account for the reality of the telecommunications supply chain where "almost everything" is manufactured "around the globe."[17] Instead, Mr. Jones has emphasized the need to view network security as "an entire system" and endorses implementation of a rigorous and comprehensive program that addresses "the full risks across the telecommunications sector."[18]

Adopting a company- or country-specific approach as the FCC proposes would provide only a false sense of security in 5G networks without any meaningful improvements in telecommunications supply chain security. As Huawei and other stakeholders have previously urged, the FCC should resist this urge and instead "support the efforts of other agencies of Government to

---

[15] *See* Julian E. Barnes and Adam Satariano, *U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist*, The New York Times (March 17, 2019), https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html.

[16] *Id.*

[17] *See* Richard Chirgwin, *Canadian Security Boss Ain't Afraid of No Huawei, Sees No Reason for Ban*, The Register (Sep. 26, 2018), https://www.theregister.co.uk/2018/09/26/canadian_security_boss_says_theres_no_reason_to_ban_huawei/; Robert Fife and Stephen Chase, *No Need to Ban Huawei in Light of Canada's Robust Cybersecurity Safeguards, Top Official Says*, The Globe and Mail (Sep. 23, 2018), *available at* https://www.theglobeandmail.com/politics/article-no-need-to-ban-huawei-in-light-of-canadas-robust-cybersecurity/.

[18] *Id.*

implement a more comprehensive, holistic approach to supply chain security that would identify and mitigate risks inherent in all manufacturers' equipment."[19]

Furthermore, imposing an equipment ban based on country of origin would likely violate the obligations imposed on members of the World Trade Organization ("WTO") and fundamental principles of the General Agreement on Tariffs and Trade not to discriminate between or against other WTO member countries in international trade. For example, Zhang Yesui, spokesman for the second session of the 13th National People's Congress, has questioned the legality of efforts by the U.S. and others to link Chinese companies to the National Intelligence Law, stating that such behavior interrupts economic activities with political means, violates the WTO rules and damages fair competition.[20] More recently, the April 11-12 meeting of the WTO's Council for Trade in Goods included discussion of the "prohibitive proposal on communication equipment or services released by the FCC" as well as Australia's "discriminatory market access prohibition on

---

[19] Written *Ex Parte* Submission of Huawei Technologies Co., Ltd and Huawei Technologies USA, Inc., WC Docket No. 18-89, at 4 (filed Mar. 12, 2019). *See also* Reply Comments of Competitive Carriers Association, Computer & Communications Industry Association, ITTA – The Voice of America's Broadband Providers, and NTCA – the Rural Broadband Association, WC Docket No. 18-89, at 9 (filed July 2, 2018) (urging the FCC to allow the Department of Homeland Security "adequate time to craft a comprehensive and holistic approach to supply chain security grounded in the principles of risk management"); Reply Comments of the Rural Wireless Broadband Coalition, WC Docket No. 18-89, at 43 (filed July 2, 2019) (advocating that the FCC work with other Federal agencies "to design and implement holistic solutions to national security threats to the nation's communications infrastructure and operations"); Reply Comments of the Rural Wireless Association, WC Docket No. 18-89, at 23-24 (filed July 2, 2019) (concurring that the FCC should coordinate with other Federal agencies on a comprehensive, holistic strategy to address supply chain risk).

[20] *See* "Highlights of news conference on NPC session," CHINA DAILY (March 4, 2019, available at: https://www.chinadailyhk.com/articles/50/144/60/1551693674782.html.

5G equipment." As a Chinese diplomat was reported to have said at the Council's meeting regarding Australia's ban on Huawei 5G equipment:

> Country-specific and discriminatory restriction measures can not address the concerns on cybersecurity, nor make anyone safe, but only disrupt the global industrial chain, and make the country itself isolated from the application of better technology.[21]

The Commission should heed these warnings and refrain from adopting its fatally flawed proposal in this proceeding. This is particularly true in light of the recent ruling that the WTO's Dispute Settlement Body and panels appointed to resolve disputes under the WTO framework may review a country's national security claims under Article XXI of the GATT 1994 to determine whether such claims have been made in good faith. In its first ruling on the GATT 1994's national security exception, the WTO Panel specifically declared that "[t]he obligation of good faith requires that members not use the exceptions in Article XXI as a means to circumvent their obligations under the GATT 1994."[22]

The Commission should not allow unsubstantiated "national security concerns" to serve as a pretext for potential violation of long-standing international trade agreements, especially since such targeted actions would fail to address supply chain security concerns effectively.

---

[21] *See* "China warns Australia at WTO about 5G restriction," REUTERS (April 15, 2019), *available at* https://www.reuters.com/article/us-huawei-australia-china-wto/china-warns-australia-at-wto-about-5g-restriction-idUSKCN1RO20H.

[22] Panel Report, Russia – Measures Concerning Traffic in Transit, para. 7.133.

Respectfully submitted,

/s/ Andrew D. Lipman

Glen D. Nager
Bruce A. Olcott
Ryan J. Watson

JONES DAY
51 Louisiana Ave, NW
Washington, D.C. 20001
(202) 879-3939
(202) 626-1700 (Fax)
gdnager@jonesday.com
bolcott@jonesday.com
rwatson@jonesday.com

Andrew D. Lipman
Russell M. Blau
David B. Salmons

MORGAN, LEWIS & BOCKIUS LLP
1111 Pennsylvania Ave, NW
Washington, DC 20004
(202) 739-3000
(202) 739-3001 (Fax)
andrew.lipman@morganlewis.com
russell.blau@morganlewis.com
david.salmons@morganlewis.com

Counsel to Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc.

June XX, 2019