Exhibit 14

9/18/2019 Huawei Ex Parte
(providing exhibits related to other telecommunications companies with connections to China)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket with additional publicly available facts about other telecommunications companies. These companies market or may wish to market telecommunications equipment and services in the United States and have substantial connections to China. This additional information further demonstrates that the Commission's proposed approach is irrational and should not be adopted.

Huawei submits as **Exhibits 1-34** documents which, taken together, demonstrate that numerous telecommunications companies have connections with China that are equally or, in many cases, more significant than those of Huawei. Some of these companies are state-owned entities; others have substantial manufacturing or other business interests in or with China, including ties between China and the two primary providers of 5G telecommunications equipment to recipients of Universal Service Fund ("USF") support. This information highlights the irrationality and arbitrariness of premising any exclusion of Huawei from the USF program on Huawei's supposed connections with China.

As Huawei has previously explained, singling out Huawei and ZTE, when numerous other companies have ties to China, demonstrates that the proposed rule is irrational and not based on any evidence that such ties present a security risk. Indeed, regarding a company as a security risk because of connections to China smacks of the invidious discrimination barred by the Constitution's equal protection guarantee. *See* Huawei Comments 44-47 (June 1, 2018). Beyond that, the Commission's proposed rule makes no reference to a company's cybersecurity-management procedures or cybersecurity risks that can come from anywhere in the supply chain. The telecommunications supply chain is global, and all major telecommunications manufacturers have operations in China, not to mention all around the world. *E.g.*, *id.* at 39-41; Huawei Reply Comments 21-22 (July 2, 2018); Huawei *Ex Parte* Submission 38 (Aug. 6, 2018). In other words, connections with China are the inevitable result of globalization; they are not a proxy for national security threats. The Commission appears to have recognized as much in other ways. For instance, the Commission has not targeted Nokia, even though Nokia (unlike Huawei) has formed a joint venture with the Chinese government. Huawei Comments 40; Huawei Reply Comments 21. That is *not* to say that the Commission should target Nokia—only that the Commission's approach is arbitrary and not based on any evidence. And even if there *were* some reason to suspect a security risk, that would not justify singling out Huawei and a handful of other companies.

The proposed rule may rest on the assumption that Chinese law or the Chinese Communist Party may require companies to spy for the Chinese state. As an initial matter, such reasoning provides no reason to single out Huawei. More importantly, though, the notion is false. As Huawei's experts have repeatedly explained, Chinese law does not permit the Chinese government to require Chinese telecommunications companies to cooperate with China's government to engage in espionage and cyberattacks. *See* Huawei Comments 43, 87-89; *id.* Ex. D (Declaration of

Ariel Lu Ye); *id.* Ex. E (Declaration of Jihong Chen & Jianwei Fang); Huawei Reply Comments 64; Huawei *Ex Parte* Submission 14-20, 36-47 (Aug. 6, 2018); Huawei *Ex Parte* Submission Ex. B (Aug. 6, 2018) (Supplemental Expert Report of Jihong Chen & Jianwei Fang); Huawei *Ex Parte* Submission & Attach. A (May 10, 2019) (Expert Report of Dr. Hanhua Zhou). Nor are Chinese companies beholden to the Communist Party. Much to the contrary, the Chinese state is bound to respect their autonomy. *See* Huawei *Ex Parte* Submission Ex. A (Aug. 6, 2018) (Expert Report of Jacques deLisle). And that makes good sense. As Huawei's expert has explained, the Chinese government would jeopardize its high-priority economic agenda by attempting to coerce leading companies like Huawei to spy for it. *Id.* at 12. For its part, Huawei too has overwhelming economic incentives to compete vigorously in the global market for telecommunications equipment and services free from any taint of complicity in state espionage efforts. *See, e.g.*, Huawei Comments Ex. L, at 10-12 (J. Suffolk, *Cyber Security Perspectives* (2012)).

Additionally, attached as **Exhibit 35** is a report regarding supply chain vulnerabilities prepared by Interos Solutions, Inc., for the U.S.-China Economic and Security Review Commission of the U.S. Government ("Interos Report"). The Interos Report identifies fifteen "entities of concern" with "relation[s] to the Chinese government" that the report claims pose supply-chain risks to U.S. information networks. The report further identifies several companies who are important suppliers of Dell and Microsoft—but not Huawei—as "present[ing] the most risk to the supply chain" as a result of their "close ties to Chinese government entities, particularly entities involved in China's military, nuclear, or cyberespionage programs."

Huawei stresses that it does not agree with the assumption by the authors of the Interos Report that substantial relationships with Chinese entities constitute any security risks to the telecommunications networks of other countries, and Huawei strongly denies any allegations—which

the report concedes are based on "unconfirmed reports"—about intellectual property theft. Huawei also does not agree with any of the other assertions about Huawei that appear in the Interos Report.

The point, rather, is that any suggestion that the U.S. Government—including the Commission—can solve supply chain issues by singling out a small number of companies for punitive treatment is profoundly misguided and will be entirely ineffective. The report demonstrates that the Commission's proposed rule is based on speculation and innuendo, not evidence.

As Huawei has previously argued, in ignoring the substantial Chinese connections of other telecommunications companies, the Commission has proposed a rule that relies on speculation, innuendo, and false assumptions rather than the realities of the global supply chain. Consequently, the proposed rule would not only punish Huawei for no reason, but it would also render the Commission's proposed rule ineffectual in achieving its stated goals of enhancing the security of the telecommunications supply chain.

Respectfully submitted,

/s/ Andrew D. Lipman

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

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

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

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

September 18, 2019

EXHIBIT LIST

Exhibit 1: "Company Profile" of Panda Electronics Group Co. Ltd.

Exhibit 2: Ericsson's "About Us: China" Webpage

Exhibit 3: "Ericsson Preserves Competitiveness on 5G Development in China"

Exhibit 4: "Ericsson: Things are Getting Better"

Exhibit 5: Excerpts from LM Ericsson Telephone Co.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Exhibit 6: Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Exhibit 7: Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year 2017

Exhibit 8: Excerpts from China Mobile Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 9: "FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S."

Exhibit 10: "Company Overview" of China Telecom (Americas)

Exhibit 11: Excerpts from China Telecom Corp. Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 12: Excerpts from China Unicom (Hong Kong) Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Exhibit 13: "Nokia Corp., Nokia and China Huaxin Sign Definitive Agreements for Creation of New Nokia Shanghai Bell Joint Venture"

Exhibit 14: "Finnish Visit to Nokia Shanghai Bell"

Exhibit 15: "NSA Concerns Give Chinese Server Maker a Boost"

Exhibit 16: PC Magazine's Online Product-Overview Page for Cisco Systems, Inc.'s Catalyst 3650-48P Layer 3 Switch

Exhibit 17: Excerpts from Cisco Systems, Inc.'s Form 10-K Annual Report for Fiscal Year Ended July 30, 2016

Exhibit 18: Excerpts from Hewlett Packard Enterprise Co.'s Form 10-K Annual Report for Fiscal Year Ended Oct. 31, 2018

Exhibit 19: "Magic Quadrant for LTE Network Infrastructure"

Exhibit 20: Excerpts from Lenovo Group Ltd.'s 2017/18 Annual Report

Exhibit 21: "USA Smartphone Market Share: By Quarter"

Exhibit 22: "DoD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices"

Exhibit 23: Backgrounder, Alcatel-Lucent Enterprise

Exhibit 24: Alpha Networks, Inc.'s "Design Manufacturing, Service (DMS)" Webpage

Exhibit 25: Alpha Networks, Inc.'s "About Alpha" Webpage

Exhibit 26: Excerpts from Arista Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year 2018

Exhibit 27: Excerpts from Extreme Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended June 30, 2018

Exhibit 28: Excerpts from Juniper Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended Dec. 31, 2018

Exhibit 29: "OnePlus Breaks Into Top 5 Premium Phone Makers in US Market"

Exhibit 30: "Who is BBK, The World's Third Largest Phone Manufacturer?"

Exhibit 31: "Meet the 'Godfather' of China's Smartphone Industry"

Exhibit 32: "China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing"

Exhibit 33: Tsinghua Holdings Co. Ltd.'s "Products and Technological Services" Webpage

Exhibit 34: "Shenzhen Government Takes Control of China's Leading Chip Maker Tsinghua Unigroup"

Exhibit 35: "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology" by Interos Solutions, Inc.

<u>Exhibit 14-A</u>

"Company Profile" of Panda Electronics Group Co. Ltd.

Click to enable Adobe Flash Player

+ Company Profile

Panda Electronics Group Company Ltd. (Panda Group) is a large comprehensive state-owned electronics enterprise with a history of over 70 years. Its business covers multiple industries including modern communications, digital audio/video and smart electronics system, electronics equipment and electronics manufacturing. Founded in 1936 and regarded as the cradle of China's electronics industry, Panda is the backbone enterprise of CEC (China Electronics Corporation).

As a key high-tech state enterprise, the Panda Group has made great contributions to national defense and modernized construction. It has been one of the top 500 enterprises for 24 consecutive years and ranked high in the top 100 electronics and IT enterprises as well as in the top 100 software enterprises. Panda brand is approved as the national famous trademark by the State Administration for Industry & Commerce of the People's Republic of China. In 1996, Nanjing Panda Electronics Company Ltd., owned by the Panda Group holding company was listed separately in the Shanghai and Hong Kong Stock Exchanges, making Panda Group the first dual-listed company in Chinese electronics industry.

Since the 1950s, more than 30 government leaders such as Mao Zedong, Deng Xiaoping, and Jiang Zemin have inspected the company, showing the sincere care and ardent hope for the development of the Panda Group. Hu Jintao, general secretary of the Central Committee of the Communist Party of China, inspected Panda Group in April, 2004, and deeply encouraged the staff to make Panda a world famous brand.

The Group has been long engaged in the innovation of core technologies with independent intellectual property rights. It has great strength in system integration and research & development in the fields of wireless communications, digital audio/video and smart information technology. It has seven national high-tech enterprises, five national engineering R&D laboratories, one post-doctoral work group and ten new product research centers. Leading science and technology personnel are developing a high standard of innovations at national and provincial institutes such as the Mobile Satellite Communication Engineering Center, the Digital Audio/Video Engineering Center, Manufacture Technology Development Center, Technology Center, Jiangsu Research Center of Optical Communication Engineering & Technology, Jiangsu Research Center of Short Wave Communications Engineering & Technology, and Jiangsu Research Center of Mobile Communication Engineering & Technology.

Panda has formed a new structure focusing on modern communications; new generation digital broadcast television and smart system equipment. With strong R&D and manufacturing capability in wireless communication field ranging from network integration and applications to terminal equipment, the Group is the national communication high-tech R&D center and an important industrial base.

In the field of civil electronics, Panda Group leads the market in providing first class domestic special communication equipment, and automatic fare collection systems, combining independent development with international cooperation. It has developed mobile communication systems including mobile communication network equipment, specific communication terminals, emergency communication and vehicular communication products, ACC/AFC rail traffic system solutions and equipment, and complete equipment for automatic mass production. With its advantages in core technologies, key processes and high-end human resources, Panda has gained increasing competitiveness.

Panda Group is also one of the largest electronics manufacturers in eastern China. With strength in manufacturing fields such as SMT, injection molding, packing, precision molding, sheet metal and digital precision mechanical machining, it provides SMT, auto-insertion of PCBs and PCBA assemblies, as well as installation, testing and maintenance services. With more than 20 advanced SMT production lines, the company has an annual production capacity of more than 15 million digital chassis and assemblies, plus over 10 billion components, 6 million LCD sets, PDP modules and complete color TVs. Panda Electronics now produces specialized plastic moldings and profiles including spray painting and auxiliary assembling. It possesses nearly 100 injection-molding machines with clamping force from 100T to 2800T.

The main joint ventures of our company are: Nanjing Ericsson Panda Communication Co., Ltd., Beijing SE Potevio Mobile Communication Co., Ltd., Nanjing Thales Panda Transportation System Co., Ltd., Nanjing LG Panda Electrical Appliance Co., Ltd. and Shenzhen Jinghua Electronics Co., Ltd.

During the period of 'The Eleventh Five-Year-Plan', the company's accumulated turnover reached RMB 130 billion and the profit and tax reached 6.8 billion, with a 22% annual sales growth rate. Its global users are up to

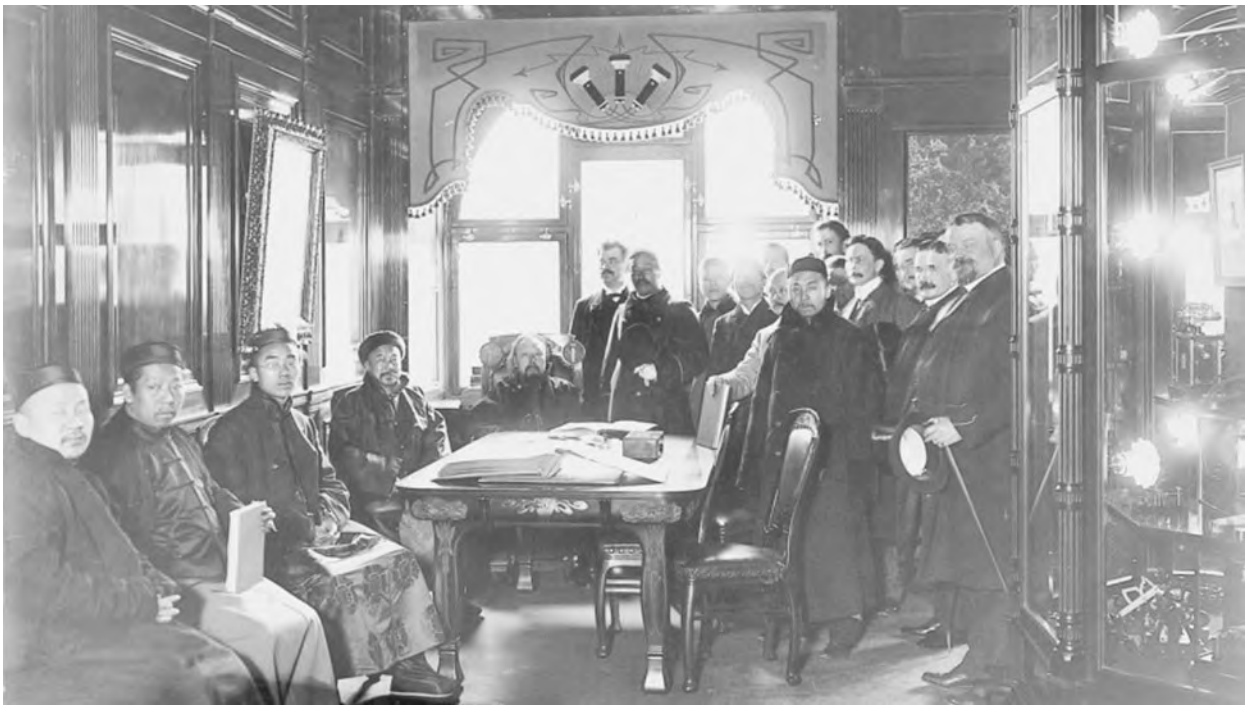
90 million.

Copyright © Panda Electronics Group Co., Ltd. All rights reserved.

<u>Exhibit 14-B</u>

Ericsson's "About Us: China" Webpage

China



Ericsson had already established a presence in China in the early 1890s through the telephone sales of Gustaf Öberg in Shanghai. Orders increased after the turn of the century when Öberg became president of a telephone operating company in the city. In 1913, Ericsson supplied equipment for a telephone station in Guangzhou (Canton). A few years later, the company also hoped to win the telephone concession in the city, but

World War I put a stop to these plans. Attempts were made again after the war but without success.

Many years would pass before Ericsson established operations in China. After the birth of the People's Republic of China in 1949 and until the death of Mao Zedong in 1976, the market was closed to Ericsson. In the late 1970s, however, the ruling Communist Party slowly began to open the enormous country to foreign companies.

At this time, Ericsson began sales of AXE stations to China. In 1985, the first representation office was opened in Beijing, and two years later, China signed what was its largest-ever telecom contract at the time for 200,000 lines of AXE.

But it was only in 1994, when Ericsson established its local company, Ericsson China Ltd, that things really took off. Just three years later, China was Ericsson's largest market with respect to order bookings.

Ericsson has several joint venture companies in China, including production companies, since the Chinese government demands local manufacturing. One important company is Nanjing Ericsson Communication Company Ltd., which was established with the electronics manufacturer Nanjing Panda Electronics. Nanjing Ericsson's accomplishments include the launch of an inexpensive mobile phone under the Panda brand that was specially developed for the Chinese market.

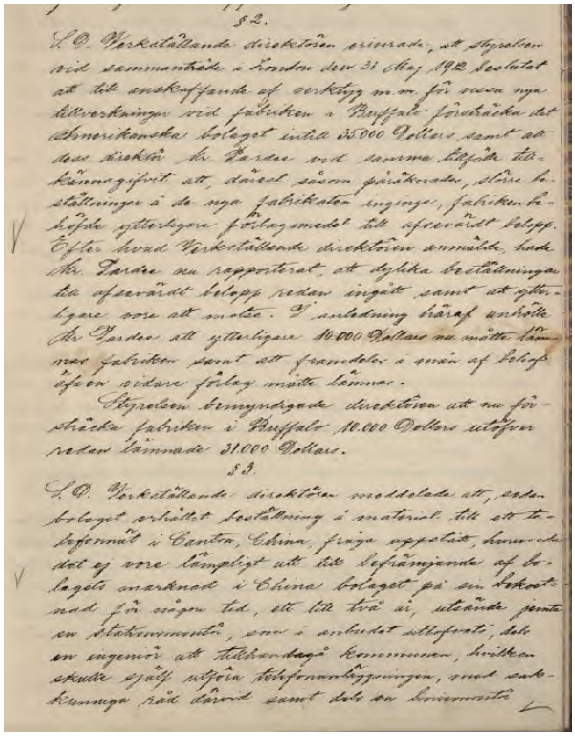
Ericsson has also invested heavily in research and training in China, which not only has its own benefits, but also provides a competitive advantage. In Shanghai, the Ericsson Communication Software Research and Development Center was established in 1997. In the same year, the Ericsson China Academy was founded in Beijing. Some 30 students are admitted each year for a two-year part-time program leading to a Master's Degree in business administration with a focus on infocom companies. Ericsson's training center in Beijing also offers shorter courses for Ericsson employees and customers.

Ericsson is assisting China in the transition from the existing digital mobile network to third-generation mobile systems. In 1999, Ericsson and the China Academy of Telecommunications Technology opened a research and development center for WCDMA technology. Together with the Beijing Institute of Technology, Ericsson has opened a research center for mobile communication.

Ericsson is particularly strong in mobile communications in China, with nearly half the market for mobile systems. With respect to fixed networks, the company's market share is about ten percent.

Author: Mats Wickman

Captain Gustaf Öberg. One of the medals is Chinese.



§ 2.

L. O. Verkställande direktören erinrade, att styrelsen vid sammanträde i London den 31 Maj 1912 beslutat att till anskaffande af verktyg m. m. för ovan nya tillverkningar vid fabriken i Buffalo förskjuta det Amerikanska bolaget intill 35.000 Dollars samt att dess direktör Mr Darden vid samma tillfälle tillkännagifvit att, därest sådan påfordrades, större beställningar i de nya fabrikaten inginge, fabriksbolaget ytterligare föreslagmedel till ofvanstående belopp. Efter hvad Verkställande direktören anmälde, hade Mr Darden nu rapporterat, att dylika beställningar till ofvanstående belopp redan ingått, samt att ytterligare voro att motse. I anledning häraf anhöll Mr Darden att ytterligare 10.000 Dollars nu måtte lämnas fabriken samt att framdeles i mån af behof öfver vidare förlag måtte lämnas.

Styrelsen bemyndigade direktören att nu förskjuta fabriken i Buffalo 10.000 Dollars utöfver redan lämnade 31.000 Dollars.

§ 3.

L. O. Verkställande direktören meddelade att, sedan bolaget erhållit beställning i material till ett telefonnät i Canton, China, finja uppsatt, denne ansett det ej vara lämpligt att till befrämjande af bolagets ansknad i China bolaget på sin bekostnad för någon tid, ett till två år, utsända jemte en installationsman, som i anbudet utlofvats, dels en ingenjör att tillhandagå kommunen, hvilken skulle sjelf utföra telefonanläggningen, med anskaffningen råd därvid samt dels en installatör

https://www.ericsson.com/en/about-us/history/places/asia/china

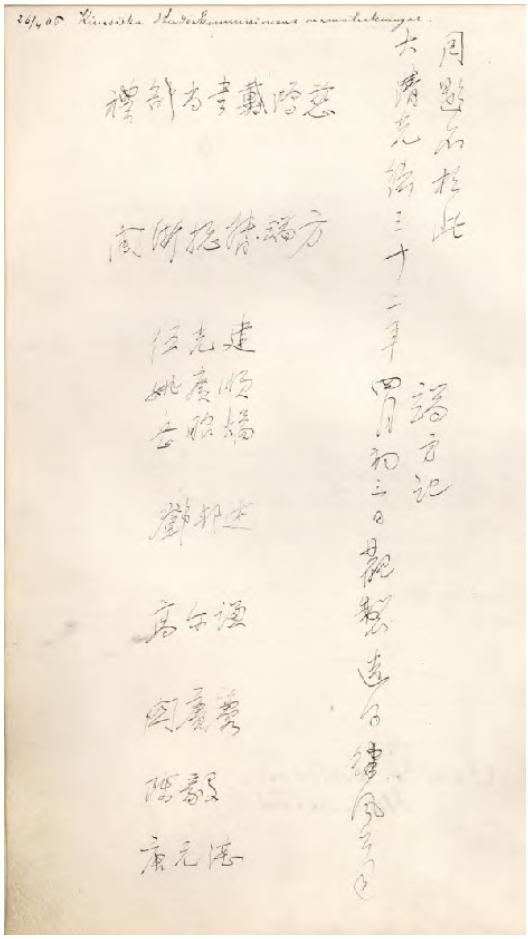
§2: The board approves a loan of USD 10,000 to the plant in Buffalo, USA.

Lars Ramqvist watching over the microscope examination of micro chips. At the inauguration of Ericsson Simtek Electronics.

Captain Gustaf Öberg dressed in Chinese clothing

https://www.ericsson.com/en/about-us/history/places/asia/china

From "The Second Better Homes and Chinese Industries Exhibition" in Shanghai, 1937. Ericsson sharing a stand with SKF, the Swedish manufacturer of ball bearings.



https://www.ericsson.com/en/about-us/history/places/asia/china

Contribute to this article

© Telefonaktiebolaget LM Ericsson and Centre for Business History

Contact info/About the site

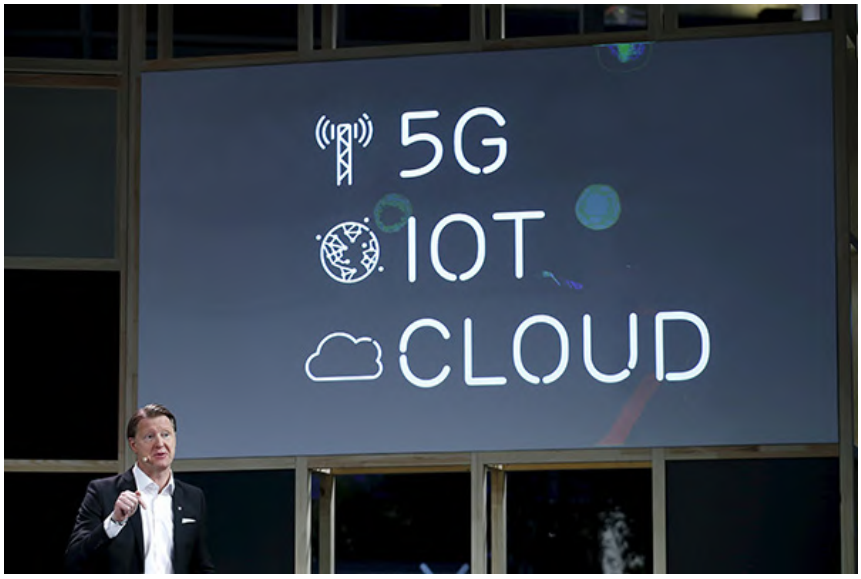
Exhibit 14-C

"Ericsson Preserves Competitiveness on 5G Development in China"

Ericsson preserves competitiveness on 5G development in China

By Liu Zheng in Barcelona, Spain (chinadaily.com.cn)

Updated: 2016-02-23 16:01



Ericsson's President & CEO Hans Vestberg attends a news conference during the Mobile World Congress in Barcelona, Spain February 22, 2016. [Photo/Agencies]

China is a strong foothold for Ericsson's research and development, manufacturing and services activities worldwide, company executive said.

"The core-competitiveness for Ericsson on 5G solutions in a market like China is that we have a full system view and we have a strong offering, consisting of both products and services, everything from the access, the transport, the cloud technologies and the complete management on the acquisition," Sara Mazur, vice president and head of Ericsson Research, told chinadaily.com.cn.

At MWC (Mobile World Congress), Ericsson President and CEO Hans Vestberg said the company has agreements with 20 major operators around the world to work together on 5G – more than any other vendor.

Vestberg pointed out that 5G radio test-bed field trials will start this year and the company is active in aligning industry time plans (3GPP, ITU-R) to assure the commercial launch of 5G in 2020.

Most Viewed Today's Top News

Top 10 most popular online shopping sites in China

Top 10 Chinese internet companies in 2017

Top 14 most powerful female billionaires in the world

Top 10 robotics companies in the world

Top 10 trading partners of the Chinese mainland

Top 10 luxury goods companies in the world

World leading internet sci-tech achievements released in Wuzhen

Top 10 most-used currencies in the world

Top 10 Chinese-listed companies with biggest brand value

Top 10 degrees that provide highest paid jobs in UK

Hot Topics

Fiat SpA Peugeot SA Taxi app

Internet finance Housing price

Disneyland 12306.cn WeChat

CHINADAILY FORUM

Daily life in Sri Lanka

Tulips in bloom in Jilin

Harmony in diversity? What does it mean?

Forest fire still burning in SW China

E China sees rare scene of dolphin group

Chinese father donates part of intestine to son

Is salary still the motive for overseas study?

Editor's Picks

Top 10 most Internet-savvy banks in China

Ericsson's 4G networks have been broadly deployed on a global scale in North and South America, the Asia Pacific region, the Middle East and Europe. To capture the next-generation ultra-faster 5G market, the vendor has ramped up research and development investments.

Ericsson's 5G wireless prototypes have taken shape, and the vendor has cooperated with major operators in Sweden, the United States, Japan, Korea and Brazil to test its 5G technology.

According to a company statement, Ericsson's annual R&D investment in China exceeds $310 million. With nearly 5,000 employees in Beijing, Shanghai, Guangzhou, Nanjing, Chengdu and Shenzhen actively engaged in R&D and product development of the entire Ericsson portfolio, China has become the largest and a truly global R&D base for Ericsson worldwide outside Sweden.

Currently, Nanjing Ericsson Panda Communication Co Ltd has grown into Ericsson's largest supply and manufacturing hub, supporting the company's global supply network and providing products for GSM, WCDMA, LTE and TD-LTE to more than 100 countries.

Ericsson is also working closely with the Chinese government, academia and the entire ecosystem in China to drive the global standardization of 5G.

On Dec 21, the company and China Mobile Research Institute (CMRI) signed a Memorandum of Understanding (MoU) to collaborate on 5G research and development.

The agreement will help drive innovation and early application of 5G mobile network technology in the country.

Under the terms of the MoU, which will initially cover a five-year period, Ericsson and China Mobile will cooperate in verification, trial and standardization of a new 5G Air Interface for commercial deployment from 2020.

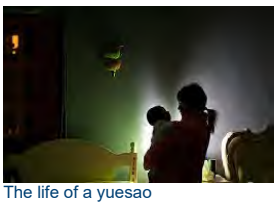
It also will closely interwork between 5G and the evolution of LTE, as well as innovate RAN features to support future industrial use cases and demonstrate, verify and conduct trials of narrowband IoT (NB-IoT) for massive machine-type communication, as well as collaboration on corresponding vertical use cases.

8.03K

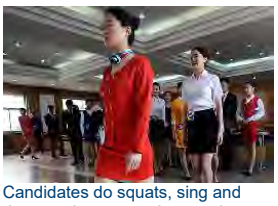
Related Stories

Ericsson reports rising income, vowing to build 5G leadership
Empowered by vision of a connected world
Ericsson aims big in China market: top executive
Ericsson reports rising sales in Q2, buoyed by China market
5G to become available by 2020: Ericsson

Photo


The life of a yuesao

Top 10 most Internet-savvy banks in China


Candidates do squats, sing and dance to become train attendants

Top 10 loss-making Chinese companies

Top 5 smart wearable vendors in the world

Top 10 overseas destinations for Chinese tourists for the holiday

Specials

World Robot Conference 2015

Made in China - fight against counterfeit goods

2015 Beijing Forum for Emerging Markets

Exhibit 14-D

"Ericsson: Things are Getting Better"

5G

Ericsson: Things are getting better

by Mike Dano | Nov 8, 2018 11:34am

Ericsson raised its 2020 sales targets. (Monica Alleven/Fierce Wireless)

Ericsson raised its 2020 sales targets due to what the company said was an improving outlook for its sales of wireless network equipment.

"With our focused strategy we have created a strong foundation of stability and profitability," Ericsson CEO Börje Ekholm **said in a statement**. "Our strengthened portfolio and competitive cost structure have enabled us to grow in the third quarter of 2018, for the first time since 2014, on a constant currency basis, despite headwind from exited contracts and businesses. As the industry moves to 5G and IoT we are now preparing to take the next step to generate profitable growth in a selective and disciplined way."

Specifically, **as noted by Reuters**, Ericsson raised its net sales goal to between $23.3 billion and $24.4 billion. The company also stuck to its target for operating margins to rise above 10% in 2020, excluding restructuring. Ericsson, though, said its longer term goal of boosting operating margins to greater than 12% would occur no later than 2022.

Ericsson said growth in its networks business "is expected to come from a stronger market, selective market shares gains, and expansion of the product portfolio into close adjacent markets. In 2019, investments in 5G trials will continue. The operating margin target for 2020 is unchanged at 15% – 17%," the company said.

Ericsson is the top provider of wireless network equipment in the United States in terms of market share, **according to research firm Dell'Oro Group**, and is listed as a major vendor for all of the country's nationwide wireless providers. And Ericsson is working to stamp out new customers as well, recently having signed network-build-out agreements with the likes of **Dish Network** and **Ligado**.

Ericsson's news also comes shortly after the company **reported** its first profitable quarter since June 2016—and after the company laid off roughly 22,000 employees. The company said net sales in North America, the company's biggest regional market behind Europe, jumped 21% year over year during the quarter and network equipment sales increased 24% in North America during the same period.

Ericsson, along with rival Nokia and other telecom equipment providers, is pinning most of its hopes on 5G, a network technology that most of the world's telecom operators hope to deploy in some fashion in the coming years.

Read More On

5G Ericsson

Suggested Articles

Wireless

CBA supports content companies' requests for C-Band safeguards

by Monica Alleven
May 15, 2019 5:03pm

Exhibit 14-E

Excerpts from LM Ericsson Telephone Co.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR (g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the Fiscal Year Ended December 31, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Commission file number 000-12033

TELEFONAKTIEBOLAGET LM ERICSSON
(Exact Name of Registrant as Specified in its Charter)

LM ERICSSON TELEPHONE COMPANY
(Translation of Registrant's name into English)

Kingdom of Sweden
(Jurisdiction of incorporation or organization)

SE-164 83 Stockholm, Sweden
(Address of principal executive offices)

Jonas Stringberg, Vice President, Head of Financial Control and Business Services
Telephone: +46 10 716 53 20, jonas.stringberg@ericsson.com
SE-164 83 Stockholm, Sweden
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange on which Registered
American Depositary Shares (each representing one B share)	The NASDAQ Stock Market LLC
B Shares *	The NASDAQ Stock Market LLC

* Not for trading, but only in connection with the registration of the American Depositary Shares representing such B Shares pursuant to the requirements of the Securities and Exchange Commission.

Securities registered pursuant to Section 12(g) of the Act:

None

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report:

B shares (SEK 5.00 nominal value)	3,072,395,752
A shares (SEK 5.00 nominal value)	261,755,983
C shares (SEK 5.00 nominal value)	0

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically, if any, every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files) Yes ☐ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer or an emerging growth company . See the definitions of "large accelerated filer" and "accelerated filer" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Emerging growth company	☐

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

☐ U.S. GAAP	☒ International Financial Reporting Standards as issued by the International Accounting Standards Board	☐ Other

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow.

Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Table of Contents

Company	Reg. No.	Domicile	Percentage of ownership	Par value in local currency, million	Carrying value, SEK million
Teleric Pty Ltd.		Australia	100	20	100
Ericsson Ltd.		China	100	2	2
Ericsson (China) Company Ltd.		China	100	65	475
Ericsson India Private Ltd.		India	67[3]	364	82
Ericsson India Global Services PVT. Ltd		India	100	291	51
Ericsson Media Solutions Ltd		Israel	100	9	51
Ericsson-LG CO Ltd.		Korea	75	285	2,279
Ericsson (Malaysia) Sdn. Bhd.		Malaysia	70	2	4
Ericsson Telecommunications Pte. Ltd.		Singapore	100	2	1
Ericsson South Africa PTY. Ltd		South Africa	70	—	135
Ericsson Taiwan Ltd.		Taiwan	90	270	36
Ericsson (Thailand) Ltd.		Thailand	49[2]	90	17
Other countries (the rest of the world)			—	—	221
Total					**71,201**
Joint ventures and associated companies					
Concealfab Co		USA	29	7	64
ST-Ericsson SA		Switzerland	50	137	—
Rockstar Consortium Group		Canada	21	1	—
Ericsson Nikola Tesla d.d.		Croatia	49	65	330
Total					**394**

1) Through subsidiary holdings, total holdings amount to 100% of Compania Ericsson S.A.C.I.
2) Through subsidiary holdings, total holdings amount to 100% of Ericsson (Thailand) Ltd.
3) Through subsidiary holdings, total holdings amount to 100% of Ericsson India Private Ltd.

Shares owned by subsidiary companies

Company	Reg. No.	Domicile	Percentage of ownership
Subsidiary companies			
Ericsson Cables Holding AB	556044-9489	Sweden	100
Ericsson France SAS		France	100
Ericsson Telekommunikation GmbH [1]		Germany	100
Ericsson Telecommunicatie B.V.		The Netherlands	100
Ericsson Telekomunikasyon A.S.		Turkey	100
Ericsson Ltd.		United Kingdom	100
Creative Broadcast Services Holdings Ltd.		United Kingdom	100
Ericsson Inc.		United States	100
Ericsson Wifi Inc.		United States	100
Redback Networks Inc.		United States	100
Telcordia Technologies Inc.		United States	83
Ericsson Telecomunicações S.A.		Brazil	100
Ericsson Australia Pty. Ltd.		Australia	100
Ericsson (China) Communications Co. Ltd.		China	100
Nanjing Ericsson Panda Communication Co. Ltd.		China	51
Ericsson Japan K.K.		Japan	100
Ericsson Communication Solutions Pte Ltd.		Singapore	100

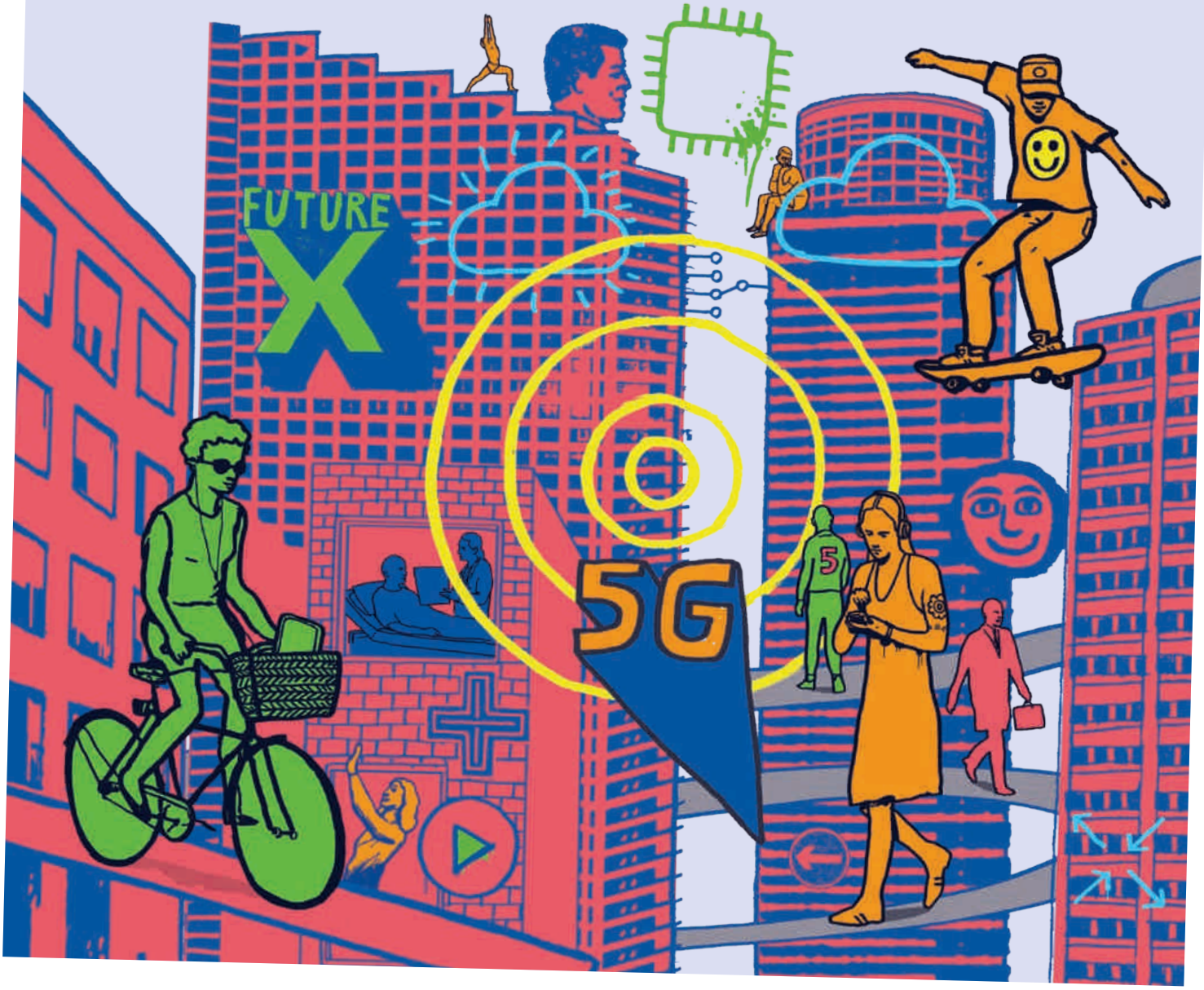
Exhibit 14-F

Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year Ended December 31, 2018

Nokia Annual Report on Form 20-F 2018

Creating the technology to connect the world

NOKIA



As filed with the Securities and Exchange Commission on March 21, 2019

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 20-F

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2018

Commission file number 1-13202

Nokia Corporation

(Exact name of Registrant as specified in its charter)

Republic of Finland
(Jurisdiction of incorporation)

Karaportti 3 FI-02610 Espoo, Finland
(Address of principal executive offices)

Esa Niinimäki, Vice President, Corporate Legal, Telephone: +358 (0) 10 44 88 000, Facsimile: +358 (0) 10 44 81 002, Karaportti 3, FI-02610 Espoo, Finland
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered pursuant to Section 12(b) of the Securities Exchange Act of 1934 (the "Exchange Act"):

Title of each class	**Name of each exchange on which registered**
American Depositary Shares	New York Stock Exchange
Shares	New York Stock Exchange[1]

(1) Not for trading, but only in connection with the registration of American Depositary Shares representing these shares, pursuant to the requirements of the Securities and Exchange Commission.

Securities registered pursuant to Section 12(g) of the Exchange Act: **None**

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Exchange Act: **None**

Indicate the number of outstanding shares of each of the registrant's classes of capital or common stock as of the close of the period covered by the annual report. Shares: **5 635 945 159**.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer", "smaller reporting company" or "emerging growth company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒ Accelerated filer ☐
Non-accelerated filer ☐ Smaller reporting company ☐
Emerging growth company ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

U.S. GAAP ☐
International Financial Reporting Standards as issued by the International Accounting Standards ☒
Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Our strategy

Our four pillars

Our strategy builds on our business portfolio and continued drive to create technology that serves people and businesses and includes the following four key priorities.

1 Lead

Lead in high-performance, end-to-end networks with CSPs

Our position

Nokia is a leader in this area today and we will use our main competitive advantage – a near-100% end-to-end portfolio that we can deliver on a global scale – to maintain our leadership while managing for profitability.

Our focus areas

- We are differentiating ourselves with our end-to-end networks that deliver benefits for our customers in automation, total cost of ownership and time to market.
- We are establishing leadership in 5G through our presence with 5G leading customers in the first 5G markets globally and achieving global technology and quality excellence.
- We are innovating in augmented intelligence, analytics and automation for fast and flawless delivery of our network infrastructure services.
- We are providing industry-leading cognitive network services to improve network performance, operational efficiency and subscriber experience, and developing service business models to open new revenue streams for CSPs.
- We are maintaining our leading market share in copper and fiber access, accelerating momentum in fixed wireless access, successfully expanding in the cable market, further developing new smart home solutions such as whole-home Wi-Fi, and simplifying network operations for our customers.
- We are leveraging our superior products and the next-generation IP routing portfolio based on our FP4 chipset to grow in both edge and core routing, where we have a fully virtualized portfolio that is differentiated by performance, flexibility, security and quality.

Progress

- We are driving the deployment of 5G: the number of customers already engaged with us on 5G is rapidly heading over the 100 mark, and amongst those we have already signed over 25 5G supply agreements. Our global base of mobile broadband customers puts us in a position of strength as 5G rollouts accelerate globally.
- In July, 2018, we announced a landmark USD 3.5 billion agreement with T-Mobile to accelerate the deployment of their nationwide 5G network in the United States. During the year we also signed three separate framework agreements with a combined value of EUR 2 billion with China Mobile, China Telecom and China Unicom.
- Independent third party assessments by P3/Connect and others testify to Nokia's superior networks performance around the world.

2 Expand

Expand network sales to select vertical markets

Our position

We continue to expand into select vertical markets that have high-performance, carrier-grade networking needs: Web and cloud companies; transportation, energy, public sector (TEPS); and TXLE (large enterprises for which technology is a strategic advantage). As the world becomes more digital and more automated, the kind of high-performance, low-latency networks once used almost exclusively in telecommunications are now needed by other organizations. This is especially true in organizations that own high-value, movable assets that are mission-critical. To address this growing need for high-performance networks, Nokia formed the Nokia Enterprise business group. With Nokia Enterprise, we have implemented a combined sales organization, a targeted portfolio and new solutions that address our customers' digitization and automation needs.

Our focus areas

- Web and cloud customers increasingly require high-performance networks to improve customer experiences and to expand their primary business models. For web and cloud companies, we are focusing on an all-IP-led approach, providing IP routing and optical network infrastructure.
- Large, tech-savvy enterprise (TXLE) customers need to virtualize and automate their hybrid cloud data centers with technology disruptions like software-defined wide area networking (SD-WAN), software-defined security, and branch office connectivity. Nokia can address those needs with SD-WAN and our all-IP portfolio.
- TEPS customers require high-performance, mission-critical networking that digitizes their energy systems, rail systems and cities. They also need to layer on top of those networks industrial automation platforms that help digitize their operations. Nokia offers mission-critical networks, solutions for digitization and Industrial IoT, and industrial automation.
- Other verticals also need to increase productivity and reduce costs through the digitization and automation of their operational systems. This can be accomplished with Industrial IoT platforms, automation platforms and private wireless networks. Nokia now targets these opportunities.

Progress

- In 2018 we made good progress in our select vertical markets with over 150 new customers and we now have more than 1 000 enterprise customers. We consolidated our enterprise-specific activities into Nokia Enterprise, our new business group, which commenced operations January 1, 2019.
- In 2018 we delivered constant currency sales growth of 9% in the enterprise space, excluding the third-party business that we are exiting, and posted solid profitability.
- We unveiled our "Future X for industries" strategy and architecture, which leverages digital transformation technologies to catalyze productivity and economic growth for enterprises.
- We also announced numerous private LTE deals during the year including Elektro, a power distributor in Brazil, and BMW's smart manufacturing facility in partnership with China Unicom.

32. Principal Group companies

The Group's significant subsidiaries as of December 31, 2018:

Company name	Country of incorporation	Parent holding %	Group ownership interest %
Nokia Solutions and Networks B.V.	Netherlands	–	100.0
Nokia Solutions and Networks Oy	Finland	100.0	100.0
Nokia of America Corporation	USA	–	100.0
Nokia Solutions and Networks India Private Limited	India	–	100.0
Nokia Technologies Oy	Finland	100.0	100.0
Alcatel-Lucent Participations SA	France	–	100.0
Nokia Canada Inc.	Canada	–	100.0
Nokia Shanghai Bell Co., Ltd[1]	China	–	50.0
Nokia Solutions and Networks Branch Operations Oy	Finland	–	100.0
Nokia Solutions and Networks Japan G.K.	Japan	–	100.0
Alcatel Submarine Networks SAS	France	–	100.0
Nokia Spain, S.A.	Spain	–	100.0
Alcatel-Lucent Italia S.p.A.[2]	Italy	–	100.0
Alcatel Lucent SAS	France	–	100.0
Nokia UK Limited	UK	–	100.0
Nokia Solutions and Networks GmbH & Co. KG	Germany	–	100.0
Alcatel-Lucent International SA	France	–	100.0
Nokia Services Limited	Australia	–	100.0
PT Nokia Solutions and Networks Indonesia	Indonesia	–	100.0
Alcatel-Lucent Brasil Telecomunicações Ltda	Brazil	–	100.0
Nokia Solutions and Networks do Brasil Telecomunicações Ltda.	Brazil	–	100.0

(1) Nokia Shanghai Bell Co., Ltd is the parent company of the Nokia Shanghai Bell joint venture of which the Group owns 50% plus one share with China Huaxin, an entity controlled by the Chinese government, holding the remaining ownership interests. Refer to Note 33, Significant partly-owned subsidiaries.
(2) Alcatel-Lucent Italia S.p.A. merged into Nokia Solutions and Networks Italia S.p.A., effective January 1, 2019.

33. Significant partly-owned subsidiaries

As part of the acquisition of Alcatel Lucent on January 4, 2016, the Group acquired a partly-owned consolidated subsidiary, Alcatel-Lucent Shanghai Bell Co., Ltd. On May 18, 2017, the Group announced the signing of definitive agreements with the China Huaxin Post & Telecommunication Economy Development Center (China Huaxin) related to the integration of Alcatel-Lucent Shanghai Bell Co,. Ltd. and the Group's China business into a new joint venture branded as Nokia Shanghai Bell.

As part of the definitive agreements, the Group transferred it's China business and subsidiaries to Nokia Shanghai Bell in exchange for a cash payment. As the transfer of the Group's China business consisted of a transaction between two Group subsidiaries, all gains or losses that arose from the transaction were fully eliminated within the Group's consolidated financial statements. Further, the transfer of cash from Nokia Shanghai Bell to the wholly-owned parent entity of the Group's China business did not impact the cash nor net cash balances in the Group's consolidated financial statements.

On July 3, 2017, the Group and China Huaxin commenced operations of the new Nokia Shanghai Bell joint venture. The Group holds an ownership interest of 50% plus one share in the Nokia Shanghai Bell's parent company, Nokia Shanghai Bell Co., Ltd., with China Huaxin holding the remaining ownership interests. The definitive agreements provide China Huaxin with the right to fully transfer its ownership interest in Nokia Shanghai Bell to the Group and the Group with the right to purchase China Huaxin's ownership interest in Nokia Shanghai Bell in exchange for a future cash settlement. As a result, the Group derecognized the non-controlling interest balance related to Nokia Shanghai Bell of EUR 772 million partly offset by the recognition of a related financial liability of EUR 737 million with the difference of EUR 35 million recorded as a gain within retained earnings as a transaction with the non-controlling interest.

The financial liability is measured based on the present value of the expected future cash settlement to acquire the non-controlling interest in Nokia Shanghai Bell. In 2018, the net present value of the expected future cash settlement amounted to EUR 693 million (EUR 672 million in 2017) and an interest expense of EUR 39 million (EUR 18 million in 2017) was recorded to reflect the recognition of the present value discount on the financial liability. In addition, the Group decreased the value of the financial liability to reflect a change in estimate of the future cash settlement resulting in the recognition of a EUR 6 million gain (EUR 64 million in 2017) in financial income and expenses in the consolidated income statement. In 2018, the Group reclassified the financial liability from non-current liabilities to current liabilities which is in line with the option exercise period.

Financial information for the Nokia Shanghai Bell Group[1]:

EURm	2018	2017
Summarized income statement		
Net sales[2]	2 518	2 276
Operating profit	54	83
Profit for the year	25	52
Profit for the year attributable to:		
Equity holders of the parent	25	15
Non-controlling interests[3]	–	37
Summarized statement of financial position		
Non-current assets	600	589
Non-current liabilities	(127)	(130)
Non-current net assets	**473**	**459**
Current assets[4]	3 340	3 888
Current liabilities	(2 209)	(2 765)
Current net assets	**1 131**	**1 123**
Net assets[5]	**1 604**	**1 582**
Non-controlling interests[6]	–	–
Summarized statement of cash flows		
Net (used in)/from operating activities	(103)	438
Net cash used in investing activities	(92)	(184)
Net cash used in financing activities	(63)	(442)
Net decrease in cash and cash equivalents	**(258)**	**(188)**

(1) Financial information for the Nokia Shanghai Bell Group is presented before eliminations of intercompany transactions with the rest of the Group but after eliminations of intercompany transactions between entities within the Nokia Shanghai Bell Group.
(2) Includes EUR 268 million (EUR 328 million in 2017) net sales to other Group entities.
(3) In 2017, profit for the year is attributed to non-controlling interests until July 3, 2017.
(4) Includes a total of EUR 738 million (EUR 1 001 million in 2017) of cash and cash equivalents and current financial investments.
(5) The distribution of the profits of Nokia Shanghai Bell Co., Ltd requires the passing of a special resolution by more than two-thirds of its shareholders, subject to a requirement that at least 50% of the after-tax distributable profits are distributed as dividends each year.
(6) In 2017, the non-controlling interest balance was derecognized and partially offset by the recognition of the related financial liability of EUR 737 million.

Exhibit 14-G

Excerpts from Nokia Corp.'s Form 20-F Annual Report for Fiscal Year 2017

Nokia Annual Report on Form 20-F 2017

Creating the technology to connect the world

As filed with the Securities and Exchange Commission on March 22, 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 20-F

ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934

For the fiscal year ended December 31, 2017

Commission file number 1-13202

Nokia Corporation

(Exact name of Registrant as specified in its charter)

Republic of Finland
(Jurisdiction of incorporation)

Karaportti 3 FI-02610 Espoo, Finland
(Address of principal executive offices)

Jussi Koskinen, Vice President, Corporate Legal, Telephone: +358 (0) 10 44 88 000, Facsimile: +358 (0) 10 44 81 002, Karaportti 3, FI-02610 Espoo, Finland
(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered pursuant to Section 12(b) of the Securities Exchange Act of 1934 (the "Exchange Act"):

Title of each class	**Name of each exchange on which registered**
American Depositary Shares	New York Stock Exchange
Shares	New York Stock Exchange[1]

(1) Not for trading, but only in connection with the registration of American Depositary Shares representing these shares, pursuant to the requirements of the Securities and Exchange Commission.

Securities registered pursuant to Section 12(g) of the Exchange Act: **None**

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Exchange Act:
5.375% Notes due 2019, 3.375% Notes due 2022, 4.375% Notes due 2027 and 6.625% Notes due 2039.

Indicate the number of outstanding shares of each of the registrant's classes of capital or common stock as of the close of the period covered by the annual report. Shares: **5 839 404 303**.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Exchange Act during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See the definitions of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒ Accelerated filer ☐
Non-accelerated filer ☐ (Do not check if a smaller reporting company) Smaller reporting company ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing:

U.S. GAAP ☐
International Financial Reporting Standards as issued by the International Accounting Standards Board ☒
Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Within our Networks business

Sales and marketing

The Customer Operations ("CO") organization is responsible for sales and account management across the five network-oriented business groups. The CO teams are represented worldwide (in approximately 130 countries) to ensure that we are close to our customers and have a deep understanding of local markets. In this way, we strive to create and maintain deep customer intimacy across our customer base.

Geographically, the CO organization is divided into seven markets:

- **Asia-Pacific and Japan** spans a varied geographical scope, ranging from advanced telecommunications markets, such as Japan and the Republic of South Korea, to developing markets including Philippines, Bangladesh, Myanmar, Vietnam and others. In 2017, we worked with all the leading operators in the market, and collaborated on 5G, IoT and other leading network evolution topics with operators from Japan and the Republic of South Korea. We also run a major Service Delivery Hub in Japan. Furthermore, we work across a wide range of vertical markets in Asia-Pacific and Japan including public sector, transportation and energy enabling solutions through its end-to-end portfolio.
- In **Europe**, we engaged with all the major operators serving millions of customers. We have extensive R&D expertise in Europe, and some of our largest Technology Centers, which are developing future technologies, are based in this market. We also have a Global Delivery Center (across two locations: Portugal and Romania) and three regional Service Delivery Hubs in Europe (one in Russia and two in Poland). With our strong end-to-end portfolio, Nokia is well positioned in Europe to help maximize the benefits of 5G, IoT and the digital transformation in the local digital ecosystems.
- In **Greater China**, we are the leading player among companies headquartered outside China, and work with all the major operators. We have also extended our market presence to the public and enterprise sectors, including energy, railways and public security. In 2017, we worked with numerous China-based webscale companies, and all the major operators in Taiwan. In China, we have six Technology Centers, one regional Service Delivery Hub and more than 80 offices spread over megacities and provinces. A major achievement in 2017 was the closing of our agreement with our Chinese partner, which resulted in the formation of the joint venture—Nokia Shanghai Bell. This was the last major organizational step in Nokia and Alcatel Lucent integration, bringing together approximately 8 000 colleagues from both companies into a single organization.
- In **India**, we are a strong supplier and service provider to the leading public and private operators. Collectively, our networks for these operators serve 418 million subscribers across some 459 000 sites with Nokia managing networks supporting 154 million subscribers. In addition, we are a key telecom infrastructure supplier to non-operator segments, including large enterprises, utilities companies, and the Indian defense sector. We are also a strategic telecommunications partner in GSM-Railways technology in India. Nokia's operations in the country include a Global Delivery Center, a Service Delivery Hub and a Global Technology Center.
- In **Latin America**, an estimated 24% of mobile subscribers use LTE services, almost double from a year ago, due to accelerated adoption in Brazil, Mexico and Argentina. High-speed fixed broadband, meanwhile, is still in its early phase. With the aim of providing broadband services to a population of over 600 million people in the area, we supplied ultra-competitive solutions to all major operators. In 2017, we also closed our biggest ever deal in the market—the nationwide wholesale LTE network in Mexico known as 'Red Compartida', for Altán Redes, and the largest LTE 700 MHz deployment in Brazil with TIM.
- In **Middle-East and Africa**, we see strong opportunities for Nokia, and we are closely working with all key global and regional operators. We have been laying the foundation for early 5G adoption and Smart Cities deployments in the Middle-East region, and continue to see strong growth in the number of mobile broadband users in Africa, driven by increasing affordability of smartphones and commercial LTE deployments across the continent.
- In **North America**, we count all the major operators as our key customers. We also deliver advanced IP networking, ultra-broadband access, and cloud technology solutions to a wide array of customers, including local service providers, cable operators, large enterprises, state and local governments, utilities, and many others. North America is also home to the our most important and thriving innovation practices—from the renowned Nokia Bell Labs headquarters in Murray Hill, New Jersey, to the development labs in Silicon Valley.

Exhibit 14-H

Excerpts from China Mobile Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, DC 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2015

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from _____ to _____

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report _____

Commission file number: 1-14696

China Mobile Limited
(Exact Name of Registrant as Specified in Its Charter)

N/A
(Translation of Registrant's Name into English)

Hong Kong, China
(Jurisdiction of Incorporation or Organization)

60th Floor, The Center
99 Queen's Road Central
Hong Kong, China
(Address of Principal Executive Offices)

Grace Wong
Company Secretary
China Mobile Limited
60th Floor, The Center
99 Queen's Road Central
Hong Kong, China
Telephone: (852) 3121-8888
Fax: (852) 2511-9092
(Name, Telephone, E-mail and/or Facsimile Number and Address of Company Contact Person)

Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange on Which Registered
Ordinary shares	**New York Stock Exchange***

* **Not for trading, but only in connection with the listing on the New York Stock Exchange of American depositary shares representing the ordinary shares.**

Securities registered or to be registered pursuant to Section 12(g) of the Act:

None
(Title of Class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report.

As of December 31, 2015, 20,475,482,897 ordinary shares were issued and outstanding.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or (15)(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Note — Checking the box above will not relieve any registrant required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 from their obligations under those Sections.

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☐ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, or a non-accelerated filer. See definition of "accelerated filer and large accelerated filer" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒ Accelerated filer ☐ Non-accelerated filer ☐

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing.

U.S. GAAP ☐ International Financial Reporting Standards as issued by the International Accounting Standards Board ☒ Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

Under our Articles of Association, our directors and senior management do not have different voting rights when compared to other holders of shares in the same class.

As of December 31, 2015, there were no outstanding options exercisable to subscribe for shares in our Company granted to our directors and members of our senior management under our share option scheme.

Item 7. Major Shareholders and Related Party Transactions.

Major Shareholders

As of March 31, 2016, approximately 72.72% of our outstanding shares were held by China Mobile Hong Kong (BVI) Limited, a wholly-owned subsidiary of China Mobile (Hong Kong) Group Limited. CMCC, a state-owned company, holds all of the voting shares and economic interest in China Mobile (Hong Kong) Group Limited. No other persons own 5% or more of our ordinary shares. Between our initial public offering and March 31, 2016, our majority shareholders held, directly or indirectly, between approximately 72.72% and 76.5% of equity interest in us, except for brief periods following our equity offerings in 1999 and 2000 but before the issuance of consideration shares to our direct shareholder, China Mobile Hong Kong (BVI) Limited, for the related acquisitions, during which periods the shareholding was temporarily lower. See “Item 4. Information on the Company — The History and Development of the Company — Industry Restructuring and Changes in Our Shareholding Structure” for changes during the past three years with respect to our majority shareholders. Under our Articles of Association, our major shareholders do not have different voting rights when compared to other holders of shares in the same class.

We are not aware of any arrangement which may at a subsequent date result in a change of control over us.

Related Party Transactions

As of March 31, 2016, CMCC indirectly owned an aggregate of approximately 72.72% of our issued and outstanding share capital.

We and each of our subsidiaries have entered into various related party transactions. The principal terms of the agreements for these related party transactions are described below.

Certain charges for the services under these agreements are based on tariffs set by the PRC regulatory authorities. Those transactions where the charges are not set by PRC regulatory authorities are based on commercial negotiation between the parties, in each case on an arm’s-length basis.

International Roaming Arrangements

Pursuant to an agreement between us and CMCC (the “International Roaming Settlement Agreement”), CMCC maintains the existing settlement arrangements with respect to international interconnection and roaming with the relevant telecommunications services providers in foreign countries and regions, and collects the relevant usage fees and other fees from us and pays the same to the relevant mobile services providers in foreign countries and regions. On September 13, 2012, we entered into an agreement with CMCC, pursuant to which CMCC would gradually transfer its settlement arrangements with certain telecommunications services providers in foreign countries and regions to China Mobile International, our wholly-owned subsidiary. As a result, our arrangement with CMCC with respect to international interconnection and roaming with those telecommunications services providers has been gradually phasing out.

Licensing of Trademark

CMCC is the owner of the “CHINA MOBILE” name and logo, a registered trademark in Mainland China, Australia, Brunei, Cambodia, Canada, Hong Kong, India, Indonesia, Macau, New Zealand, Pakistan, South Africa, South Korea, Taiwan, Thailand, the United States and Yemen. In addition, it has filed applications to register the “CHINA MOBILE” name and logo as a trademark in Malaysia for certain goods and services. CMCC has also registered the “CHINA MOBILE” name and logo as a trademark under the Protocol Relating to the Madrid Agreement Concerning the International Registration of Marks.

Exhibit 14-I

"FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S."

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/fcc-denies-china-mobiles-bid-to-provide-international-telecom-services-in-the-u-s-11557416760

BUSINESS

FCC Denies China Mobile's Bid to Provide International Telecom Services in the U.S.

Regulators cited a review that determined Chinese state ownership of the company posed national security and law enforcement risks

A staffer for the Federal Communications Commission said Thursday that China Mobile is "subject to exploitation, influence and control by the Chinese government." PHOTO: SERGIO PEREZ/REUTERS

By Ryan Tracy

Updated May 9, 2019 1:33 p.m. ET

WASHINGTON—The U.S. blocked a Chinese telecom giant from providing services via American networks, the latest sign of escalating tension between the two global powers.

The Federal Communications Commission voted unanimously to deny an application by China Mobile Ltd.'s U.S. arm, China Mobile USA, to provide international calls and other services. U.S. officials cited law enforcement and national security risks, saying the company is owned by the Chinese government and vulnerable to exploitation, influence and control.

"The Chinese government could use China Mobile to exploit our telephone network to increase intelligence collection against U.S. government agencies and other sensitive targets that depend on this network," FCC Chairman Ajit Pai said. "That is a flatly unacceptable risk."

The FCC's denial comes at a sensitive time, with the two countries in the final stages of negotiating a difficult trade deal and financial markets on edge over the prospect of a deteriorating China-U.S. relationship. China Mobile is by some measures the world's largest

mobile telecommunications firm. The parent company didn't immediately respond to an email requesting comment Thursday.

In a May 1 letter to the commission, an attorney representing China Mobile said it "continues to believe that this action is guided more by tensions in the bilateral U.S.-China relationship than an absence of" options to mitigate regulators' concerns.

The FCC's 5-0 vote underscored bipartisan concern about the application, originally filed in 2011. The expected move came after a yearslong review by U.S. agencies recommended in July 2018 that the FCC deny China Mobile's request.

It was the first time the U.S. government has recommended denying an application to provide telecom services based on national security and law enforcement concerns, the FCC said. The agencies determined China Mobile USA "would likely comply with espionage and intelligence requests made by the Chinese government," according to the FCC.

The FCC could go further. Mr. Pai said the agency is reviewing whether two other Chinese telecom firms, operating in the U.S., should retain permits.

"Security threats have evolved over the many years since those companies were granted interconnection rights to U.S. networks in the early 2000s," said FCC Commissioner Brendan Carr said.

The decision was the latest of the Trump administration's efforts to block Chinese firms from gaining control of U.S. companies in technology and other sectors. Earlier this year, the U.S. ordered Beijing Kunlun Tech Co. Ltd to sell its majority stake in the dating app Grindr, citing the risk that the personal data collected via the app could be use to blackmail individuals with U.S. security clearances, The Wall Street Journal reported in March.

Last year, U.S. regulators blocked the sale of the Chicago stock exchange to a group that would have included Chinese investors.

China Mobile is considered a state-owned enterprise, but also is listed on the New York Stock Exchange and in Hong Kong.

Write to Ryan Tracy at ryan.tracy@wsj.com

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

Exhibit 14-J

"Company Overview" of China Telecom (Americas)

CHINA TELECOM AMERICAS

Company Overview

Headquartered in Herndon, Virginia, China Telecom Americas is the largest international subsidiary of China Telecom Corporation Limited, as well as the only authorized re-seller of domestic Chinese telecom products to North American companies. China Telecom Americas has offices in 31 countries, providing access to Chinese telecom network assets for customers in the United States, Canada and Latin America.

As the largest operating broadband operator in the world (127 million subscribers), as well as the world's largest CDMA mobile operator (227 million subscribers), China Telecom delivers a comprehensive global telecom service scope based on cutting edge technology, exceptional customer service, and a visionary approach to international telecommunications.

- **Key Facts**
- **Mission**
- **About China Telecom Global**
- **About China Telecom Corporation**

China Telecom's core strengths in facts & figures:

- World's largest fixed line operator (144 million fixed access lines in service).
- World's largest broadband operator (127 million subscribers)
- World's largest CDMA mobile operator (227 million subscribers, including 147 million 4G subscribers)
- Owns and operates China's largest optical fiber network: over 83,000 km long, covering 70% of China's territory and connecting all Chinese cities
- Owns and operates ChinaNet, China's largest Internet network
- Owns and operates China's largest MPLS VPN network, based on CN2, our next-generation, carrier-class, IPv6-capable Internet backbone network
- Primary service provider in all 21 southern provinces in China.
- Owns comprehensive trans-Pacific cable systems, including China-U.S., Japan-U.S., SEA-ME-WE3 in APCN2, SMW3, SMW5, FASTER, Flag, TAE, etc.
- International bilateral connectivity to 100+ countries
- More than 670,000 professionals employed around the world

- Ranked #132 on Fortune's Global 500 in 2016.

Latest News

- China Telecom, Tata Communications Partner to drive global connectivity for IoT devices
- China Telecom Backs Launch of GSMA's Digital Declaration at Davos
- Sharktech Adds China Telecom CN2 to Los Angeles Network Offering
- Keysight Technologies, China Telecom Collaborate To Accelerate Commercial Deployment Of 5G Technology
- Breakthrough for "the Belt and Road Initiative" project, China Telecom completes the first direct access optical fibe...

MORE NEWS

Insights

- China Telecom Implements a Low Voltage System for Minghua's $45 million Spartanburg plant
- China Telecom, Shenzhen Water Group Deliver the World's First Commercial NB-IoT-based Water Management Platform
- China Telecom Showcases Smart Waste Management Platform at the 2017 World Internet Conference in Wuzhen, China
- The Benefits of SD-WAN for a Globalized IT Economy
- China Data Center Trends and Future Outlook

MORE INSIGHTS

Events

- JUNE 9 - 13, 2019**Cisco Live**San Diego, CA | Booth 3532
- APRIL 9 - 12, 2019**Channel Partners**Las Vegas, NV | Booth 344
- APRIL 9 - 11, 2019**Google Cloud Next '19**San Francisco, CA
- APRIL 8 - 9, 2019**WAN Summit 2019**New York, NY | Table Number 6
- MARCH 10-13, 2019**Super9 Convergence**Nashville, TN | Table #24

https://www.ctamericas.com/company/company-overview/

Contact Us

Questions about which solutions are right for your organization? We can help!

Exhibit 14-K

Excerpts from China Telecom Corp. Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, DC 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report

For the transition period from to

Commission file number 1-31517

中国电信股份有限公司

(Exact Name of Registrant as Specified in Its Charter)

China Telecom Corporation Limited

(Translation of Registrant's Name into English)

People's Republic of China

(Jurisdiction of Incorporation or Organization)

31 Jinrong Street, Xicheng District
Beijing, People's Republic of China 100033

(Address of Principal Executive Offices)

Ms. Wong Yuk Har, Rebecca
China Telecom Corporation Limited
28/F, Everbright Centre
108 Gloucester Road
Wanchai, Hong Kong
Email: rebecca.wong@chinatelecom-h.com
Telephone: (+852) 2582 5819
Fax: (+852) 2157 0010

(Name, Telephone, E-mail and/or Facsimile number and Address of Company Contact Person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange On Which Registered
American depositary shares	New York Stock Exchange, Inc.
H shares, par value RMB1.00 per share	New York Stock Exchange, Inc.*

* Not for trading, but only in connection with the listing on the New York Stock Exchange, Inc. of American depositary shares, each representing 100 H shares.

Securities registered or to be registered pursuant to Section 12(g) of the Act:

None
(Title of Class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:
None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report.

As of December 31, 2018, 67,054,958,321 domestic shares and 13,877,410,000 H shares, par value RMB1.00 per share, were issued and outstanding. H shares are ordinary shares of the Company listed on The Stock Exchange of Hong Kong Limited.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files) Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or an emerging growth company. See definition of "large accelerated filer," "accelerated filer," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer ☒ Accelerated Filer ☐ Non-Accelerated Filer ☐ Emerging Growth Company ☐

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards† provided pursuant to Section 13 (a) of the Exchange Act. ☐

† The term "new or revised financial accounting standard" refers to any update issued by the Financial Accounting Standards Board to its Accounting Standards Codification After April 5, 2012.

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing.

U.S. GAAP ☐

International Financial Reporting Standards as issued by the International Accounting Standards Board ☒

Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow. Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

(APPLICABLE ONLY TO ISSUERS INVOLVED IN BANKRUPTCY PROCEEDINGS DURING THE PAST FIVE YEARS)

Indicate by check mark whether the registrant has filed all documents and reports required to be filed by Sections 12, 13 or 15(d) of the Securities Exchange Act of 1934 subsequent to the distribution of securities under a plan confirmed by a court. Yes ☐ No ☐

We cannot assure you that we can obtain sufficient financing at commercially reasonable terms or at all. If adequate capital is not available on commercially reasonable terms, our growth potential and prospects could be materially and adversely affected. Furthermore, additional issuances of equity securities will result in dilution to our shareholders. Incurrence of debt would result in increased interest expense and could require us to agree to restrictive operating and financial covenants.

If we are not able to respond successfully and cost-efficiently to technological or industry developments, our business may be materially and adversely affected.

The telecommunications market is characterized by rapid advancements in technology, evolving industry standards and changes in customer needs. We cannot assure you that we will be successful in responding to these developments. In addition, new services or technologies, such as mobile Internet, the three-network convergence, cloud computing and Internet of Things, may render our existing services or technologies less competitive. In the event we do take measures to respond to technological developments and changes in industry standards, the integration of new technology or industry standards or the upgrading of our networks may require substantial time, effort and capital investment. Moreover, the successful deployment and application of such cutting edge technologies depend on a number of factors, including the integration of legacy networks and cloud security related challenges. We cannot assure you that we will succeed in integrating these new technologies and industry standards or adapting our network and systems in a timely and cost-effective manner, or at all. Our inability to respond successfully and cost-efficiently to technological or industry developments may materially and adversely affect our business, results of operations and competitiveness.

Our ability to respond to technological developments in a cost-efficient manner may also be adversely affected by external factors, some of which are beyond our control. For example, the development in 5G technology is expected to have a major impact on our services. We have been engaged in standards formulation, network technology trial runs as well as planning of the application of 5G services towards commercialization. In December 2018, China Telecom Group was granted the approval from the MIIT to utilize the 3400-3500MHz spectrum nationwide for 5G system trial until June 30, 2020. In addition, we have been taking the initiatives to explore the feasibility of collaborative development of 5G and 4G. We have devoted, and will continue to devote, substantial resources in the development of 5G technology. However, various details concerning 5G services are still uncertain, including the timing of the issuance of 5G permits, the frequency bands allocated to 5G services and relevant regulations. In addition, there is no assurance that we will be able to roll out 5G services in an economically viable manner to gain favorable market share based on reasonable commercial terms with business partners without undue delay. Furthermore, the 5G industry chain is still under development, and we continue to explore 5G services' business model and commercial applications. If we are unable to respond to these uncertainties, the expected benefits from our investment in development of 5G technology would not be fully realized or at all and such inability to respond to these uncertainties may materially and adversely affect our business in the future.

We are subject to risks associated with our telecommunications equipment suppliers and other business partners which could be adversely affected by restrictions, sanctions or other legal or regulatory actions under relevant laws and regulations in various jurisdictions which in turn could adversely affect the supply chain and our business operations.

We procure our telecommunications network equipment and related maintenance and technical support from certain PRC and overseas telecommunications equipment suppliers. See "Item 4. Information on the Company—B. Business Overview—Network System". We also transact business with our business partners who may operate globally. As these parties operate globally and are therefore subject to the laws and regulations in various jurisdictions, any restrictions, sanctions or other legal or regulatory actions could cause disruptions or other material difficulties in their business activities to the extent any government of the relevant jurisdictions imposes any restrictions on their import and export activities, or sanctions or other legal or regulatory actions against the suppliers and other business partners in connection with their business activities. The relevant jurisdictions include, among others, the United States, the European Union and the United Nations. Furthermore, as the supply of our telecommunications equipment relies on a global supply chain, which is vulnerable to significant disruptions in the supply of parts and other items that are necessary for the relevant manufacturing activities. Such disruptions could prevent those affected suppliers from delivering equipment and services to us in accordance with the agreed terms of supply, which in turn could negatively affect our business operations. For example, we may not be able to find suitable alternative suppliers for the affected equipment in a timely manner. Even if we are able to find alternative suppliers, the commercial terms may not be comparable, and we could therefore be subject to a higher procuring cost. Furthermore, if any of our suppliers raises their prices due to an increase in international trade tariffs, we could be subject to a higher cost in procuring the relevant products. We may experience a significant delay in implementing the part of our business plans that relies on delivery of the affected network equipment and difficulties in timely improving our services that rely on those suppliers for upgrading our networks and related software and applications. Any of these and other consequences could materially adversely affect our business, results of operations, financial condition and prospect and cause a significant volatility in and a decline in our share price.

Universal Services

Under the Telecommunications Regulations, telecommunications service providers in the PRC are required to fulfill universal service obligations in accordance with relevant regulations promulgated by the PRC government, and the MIIT has been given authority by the PRC government to delineate the scope of its universal service obligations. The MIIT, together with other regulatory authorities, is also responsible for formulating administrative rules relating to the establishment of a universal service fund and compensation schemes for universal services. The State Council issued the Notice on the "Broadband China" Policy and the Implementation Plan on August 1, 2013, which included the provision of broadband services to remote villages as part of the universal service obligations of telecommunications service providers and mentioned improving the compensation scheme for the expenses incurred in the "Broadband China" projects undertaken by telecommunications service providers in the villages. In addition, the MOF and the MIIT jointly issued the Notice of Implementation of Telecommunications Universal Services Pilot Work in December 2015, which provided that the telecommunications universal services should take a market-oriented approach and that the telecommunications universal services providers should be selected through a public bidding process. This notice sets up certain goals for the telecommunications operators, including broadband coverage in 98% of the administrative villages and over 12Mbps broadband access capacity in rural villages, by 2020. Pursuant to the notice, the central government subsidies will be granted to the pilot areas determined by the MOF and the MIIT and the universal services providers will be selected through an open bidding process.

The PRC government used financial resources to compensate the expenses incurred in the "Coverage to All Villages" and the "Broadband China" projects before the implementation of universal services pilot projects in 2016. We, together with other telecommunications operators, have undertaken the "Coverage to All Villages" project since 2004. Since 2016, we have undertaken universal services pilot projects in accordance with the requirements of the Chinese government and in aggregate won the bids to undertake the construction of broadband network facilities in approximately 50,000 administrative villages in 19 provinces and autonomous regions. By the end of 2018, we had completed the construction of broadband networks in approximately 50,000 administrative villages. Since 2018, the PRC government included 4G network coverage into the scope of pilot projects for universal services. We have continuously promoted the construction of communication networks in rural areas and remote rural villages and strives to improve the broadband access coverage in rural areas. In addition, we have set up local service points for rural villages, actively promoted the development of e-commerce in rural areas, and strived to contribute to the informatization upgrade and revitalization of rural areas in various regions. The compensation from the PRC government may not be sufficient to cover all of our expenses for providing the telecommunications universal services. However, we believe the expenses for such operation and maintenance will not have a material effect on our financial condition.

State-Owned Assets Supervision

Under the PRC Company Law, PRC Enterprise State-Owned Assets Law, Interim Measures for the Supervision and Administration of State-Owned Assets of the Enterprises, and other administrative regulations, the SASAC, among others, supervises the preservation of the value of state-owned assets, guides the reform and restructuring of state-owned enterprises, and evaluates the performance of management executives of state-owned enterprises through legal procedures. Our controlling shareholder, China Telecom Group, is a state-owned enterprise owned by the SASAC and subject to the SASAC's supervision.

As part of the PRC government's efforts to reform state-owned enterprises and increase their competitiveness, the PRC government has selected certain enterprises of designated industries, including the telecommunications industry, as the first group of state-owned enterprises for a pilot program on state-owned enterprise mixed ownership reform. Unicom Group was selected among the operators of the telecommunications industry to join such mixed ownership reform.

Three-Network Convergence Policy

In January 2010, the PRC government announced its decision to accelerate the advancement of convergence of telecommunications, television broadcast and Internet access networks to realize interconnection and resource co-sharing among the three networks and further develop the provision of voice, data, television and other services. Specifically, the three-network convergence policy will be initially carried out on a trial basis in selective geographic locations during the period from 2010 to 2012 and further implemented across-the-board in the following three years. In June 2010, the State Council issued the Trial Plan for Three-Network Convergence and called for 12 volunteer regions (cities) and enterprises for the first trial. Following the completion of the first trial in December 2011, the State Council announced 42 additional regions (cities) for the second phase of the trial. In September 2012, we received the Information Network Communicated Audio-Video Program License from the State Administration of Press, Publication, Radio, Film and Television (the "SARFT", formerly, the State Administration of Radio, Film and Television). In August 2015, the General Office of the State Council issued the Notice of Plan of Furthering the Three-Network Convergence, which marked the completion of the trial plan of the three-network convergence and called for furthering the three-network convergence nationwide.

36. RECONCILIATION OF LIABILITIES ARISING FROM FINANCING ACTIVITIES

The table below details changes in the Group's liabilities arising from financing activities, including both cash and non-cash changes. Liabilities arising from financing activities are those for which cash flows were, or future cash flows will be, classified in the Group's consolidated statement of cash flows as cash flows from financing activities.

	Short-term Debt RMB	Long-term debt and payable RMB	Finance lease obligation RMB	Other payables in respect of the reduction of capital by non-controlling interests RMB	Consideration payable in respect of the Eighth Acquisition (Note 20) RMB	Consideration payable in respect of the acquisition of non-controlling interests (Note 20) RMB	Dividend payable RMB	Total RMB
Balance as of January 1, 2017	40,780	71,646	102	—	—	—	—	112,528
Financing cash flows	13,778	(22,191)	(84)	—	—	(31)	(7,619)	(16,147)
New finance leases	—	—	55	—	—	—	—	55
Interest expenses	—	295	9	—	—	—	—	304
Foreign exchange gain	—	(8)	—	—	—	—	—	(8)
Acquisition of the Eighth Acquired Group	—	—	—	—	87	—	—	87
Acquisition of non-controlling interests	—	—	—	—	—	150	—	150
Distribution to non-controlling interests	—	—	—	—	—	—	89	89
Dividends declared	—	—	—	—	—	—	7,530	7,530
Others	—	—	(5)	—	—	—	—	(5)
Balance as of December 31, 2017	54,558	49,742	77	—	87	119	—	104,583
Financing cash flows	(5,021)	(4,073)	(73)	(20)	(87)	(119)	(7,745)	(17,138)
New finance leases	—	—	200	—	—	—	—	200
Interest expenses	—	304	12	—	—	—	—	316
Foreign exchange loss	—	18	—	—	—	—	—	18
Reduction of capital by non-controlling interests	—	—	—	20	—	—	—	20
Distribution to non-controlling interests	—	—	—	—	—	—	177	177
Dividends declared	—	—	—	—	—	—	7,568	7,568
Balance as of December 31, 2018	49,537	45,991	216	—	—	—	—	95,744

Other than net financing cash outflows for the year ended December 31, 2018 totaling RMB17,138 as presented above, E-surfing Pay, a subsidiary of the Company, received RMB855 in the current year as part of the consideration amounting to RMB945 in respect of contribution from non-controlling interests. The remaining balance of RMB90 as of December 31, 2018 was included in prepayments and other current assets (Note 8).

37. RELATED PARTY TRANSACTIONS

(a) Transactions with China Telecom Group

The Group is a part of companies under China Telecommunications Corporation, a company owned by the PRC government, and has significant transactions and business relationships with members of China Telecom Group.

The principal transactions with China Telecom Group which were carried out in the ordinary course of business are as follows.

	Notes	Year ended December 31, 2016 RMB	2017 RMB	2018 RMB
Construction and engineering services.	(i)	18,936	18,672	16,396
Receiving ancillary services.	(ii)	13,938	16,072	16,744
Interconnection revenues	(iii)	60	48	80
Interconnection charges	(iii)	232	193	204
Receiving community services	(iv)	2,871	3,028	3,296
Net transaction amount of centralized services	(v)	523	727	519
Property lease income	(vi)	36	53	48
Property lease expenses	(vi)	559	654	713
Provision of IT services	(vii)	312	642	531
Receiving IT services	(vii)	1,597	1,812	1,895
Purchases of telecommunications equipment and materials.	(viii)	5,199	4,248	3,760
Sales of telecommunications equipment and materials.	(viii)	2,786	3,291	2,760
Internet applications channel services	(ix)	332	344	298
Interest on amounts due to and loans from China Telecom Group	(x)	2,928	2,720	2,099
Others	(xi)	176	190	186

39. SHARE APPRECIATION RIGHTS (continued)

In November 2018, the Company approved the granting of 2,394 million share appreciation right units to eligible employees. Under the terms of this grant, all share appreciation rights had a contractual life of five years from date of grant and an exercise price of HK$3.81 per unit. A recipient of share appreciation rights may exercise the rights in stages commencing November 2020. As of each of the third, fourth and fifth anniversary of the date of grant, the total number of share appreciation rights exercisable may not in aggregate exceed 33.3%, 66.7% and 100.0%, respectively, of the total share appreciation rights granted to such person.

During the year ended December 31, 2018 and 2017, no share appreciation right units were exercised. For the year ended December 31, 2018, compensation expense of RMB30 was recognized by the Group in respect of share appreciation rights (2017: Nil).

As of December 31, 2018, the carrying amount of the liability arising from share appreciation rights was RMB30. As of December 31, 2017, no liability arising from share appreciation rights was assumed by the Group.

40. PRINCIPAL SUBSIDIARIES

Details of the Company's subsidiaries which principally affected the results, assets and liabilities of the Group as of December 31, 2018 are as follows:

Name of company	Type of legal entity	Date of incorporation	Place of incorporation and operation	Registered /issued capital (in RMB million unless otherwise stated)	Principal activities
China Telecom System Integration Co., Limited	Limited Company	September 13, 2001	PRC	542	Provision of system integration and consulting services
China Telecom Global Limited	Limited Company	February 25, 2000	Hong Kong Special Administrative Region of the PRC	HK$168 million	Provision of telecommunications services
China Telecom (Americas) Corporation	Limited Company	November 22, 2001	The United States of America	US$43 million	Provision of telecommunications services
China Telecom Best Tone Information Service Co., Limited	Limited Company	August 15, 2007	PRC	350	Provision of Best Tone information services
China Telecom (Macau) Company Limited	Limited Company	October 15, 2004	Macau Special Administrative Region of the PRC	MOP60 million	Provision of telecommunications services
Tianyi Telecom Terminals Company Limited	Limited Company	July 1, 2005	PRC	500	Sales of telecommunications terminals
China Telecom (Singapore) Pte. Limited	Limited Company	October 5, 2006	Singapore	S$1,000,001	Provision of international value-added network services
E-surfing Pay Co., Ltd	Limited Company	March 3, 2011	PRC	500	Provision of e-commerce service
Shenzhen Shekou Telecommunications Company Limited	Limited Company	May 5, 1984	PRC	91	Provision of telecommunications services
China Telecom (Australia) Pty Ltd	Limited Company	January 10, 2011	Australia	AUD1 million	Provision of international value-added network services
China Telecom Korea Co.,Ltd	Limited Company	May 16, 2012	South Korea	KRW500 million	Provision of international value-added network services
China Telecom (Malaysia) SDN BHD	Limited Company	June 26, 2012	Malaysia	MYR3,723,500	Provision of international value-added network services
China Telecom Information Technology (Vietnam) Co., Ltd	Limited Company	July 9, 2012	Vietnam	VND10,500 million	Provision of international value-added network services
iMUSIC Culture & Technology Co., Ltd.	Limited Company	June 9, 2013	PRC	250	Provision of music production and related information services
China Telecom (Europe) Limited	Limited Company	March 2, 2006	The United Kingdom of Great Britain and Northern Ireland	GBP16.15 million	Provision of international value-added network services
Zhejiang Yixin Technology Co., Ltd.	Limited Company	August 19, 2013	PRC	11	Provision of instant messenger service
Tianyi Capital Holding Co., Ltd.	Limited Company	November 30, 2017	PRC	5,000	Capital Investment and provision of consulting services
China Telecom Leasing Corporation Limited.	Limited Company	November 30, 2018	PRC	5,000	Provision of finance lease service

Exhibit 14-L

Excerpts from China Unicom (Hong Kong) Ltd.'s Form 20-F Annual Report for Fiscal Year 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 20-F

☐ **REGISTRATION STATEMENT PURSUANT TO SECTION 12(b) OR 12(g) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

OR

☐ **SHELL COMPANY REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

Date of event requiring this shell company report _____

For the transition period from _____ to _____

Commission file number 1-15028

CHINA UNICOM (HONG KONG) LIMITED
(Exact Name of Registrant as Specified in Its Charter)

N/A
(Translation of Registrant's Name Into English)

Hong Kong
(Jurisdiction of Incorporation or Organization)

75th Floor, The Center
99 Queen's Road Central
Hong Kong
(Address of Principal Executive Offices)

Yung Shun Loy Jacky
Telephone: +852 2121 3220
Facsimile: +852 2121 3232
75th Floor, The Center
99 Queen's Road Central
Hong Kong
(Name, Telephone, E-mail and/or Facsimile Number and Address of Company Contact person)

Securities registered or to be registered pursuant to Section 12(b) of the Act:

Title of Each Class	Name of Each Exchange On Which Registered
Ordinary shares	**The New York Stock Exchange, Inc.***

* Not for trading, but only in connection with the listing on The New York Stock Exchange, Inc. of American depositary shares, or ADSs, each representing 10 ordinary shares.

Securities registered or to be registered pursuant to Section 12(g) of the Act:

None
(Title of class)

Securities for which there is a reporting obligation pursuant to Section 15(d) of the Act:

None
(Title of Class)

Indicate the number of outstanding shares of each of the issuer's classes of capital or common stock as of the close of the period covered by the annual report.

As of December 31, 2018, 30,598,124,345 ordinary shares were issued and outstanding.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

If this report is an annual or transition report, indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934. Yes ☐ No ☒

Note – Checking the box above will not relieve any registrant required to file reports pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 from their obligations under those Sections.

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 (§232.405 of this chapter) of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," and "emerging growth company" in Rule 12b-2 of the Exchange Act

Large accelerated filer ☒ Accelerated filer ☐ Non-accelerated filer ☐ Emerging growth company ☐

If an emerging growth company that prepares its financial statements in accordance with U.S. GAAP, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards† provided pursuant to Section 13 (a) of the Exchange Act. ☐

† The term "new or revised financial accounting standard" refers to any update issued by the Financial Accounting Standards Board to its Accounting Standards Codification after April 5, 2012.

Indicate by check mark which basis of accounting the registrant has used to prepare the financial statements included in this filing.

U.S. GAAP ☐ International Financial Reporting Standards as issued by the International Accounting Standards Board ☒ Other ☐

If "Other" has been checked in response to the previous question, indicate by check mark which financial statement item the registrant has elected to follow.

Item 17 ☐ Item 18 ☐

If this is an annual report, indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

(APPLICABLE ONLY TO ISSUERS INVOLVED IN BANKRUPTCY PROCEEDINGS DURING THE PAST FIVE YEARS)

Indicate by check mark whether the registrant has filed all documents and reports required to be filed by Sections 12, 13 or 15(d) of the Securities Exchange Act of 1934 subsequent to the distribution of securities under a plan confirmed by a court. Yes ☐ No ☐

	As of or for the year ended December 31,					
	2014	2015	2016	2017	2018	2018
	RMB	RMB	RMB	RMB	RMB	US$[1]
	(in millions, except for per share data)					
Other Financial Data:						
Net cash inflow from operating activities	88,904	84,301	74,593	85,054	92,387	13,437
Net cash outflow from investing activities	(75,319)	(91,354)	(95,749)	(47,336)	(61,179)	(8,898)
Net cash (outflow)/inflow from financing activities	(8,973)	3,427	22,877	(28,414)	(34,058)	(4,954)
Net increase/(decrease) in cash and cash equivalents	**3,802**	**(3,626)**	**1,721**	**9,304**	**(2,850)**	**(415)**
Dividend declared per share	**0.20**	**0.17**	**—**	**0.052**	**0.134**	**0.019**

(1) The translation of RMB into U.S. dollars has been made at the rate of RMB6.8755 to US$1.00, representing the exchange rate as set forth in the H.10 statistical release of the Federal Reserve Board on December 31, 2018. The translations are solely for the convenience of the reader.

(2) Revenue from sales of products associated with the ICT business, which was previously recorded as part of the fixed-line service revenue, has been reclassified as revenue from sales of telecommunications products since 2017 to better reflect the commercial nature of the transactions. The related figures for the years ended December 31, 2014, 2015 and 2016 have been reclassified on the same basis.

(3) See Note 14 to our consolidated financial statements included elsewhere in this annual report on Form 20-F on how basic and diluted earnings per share are calculated under IFRS.

(4) Earnings per ADS is calculated by multiplying earnings per share by 10, which is the number of shares represented by each ADS.

B. Capitalization and Indebtedness

Not Applicable.

C. Reasons for the Offer and Use of Proceeds

Not Applicable.

D. Risk Factors

Risks Relating to Our Business

We face intense competition from other telecommunications operators, including China Mobile and China Telecom, and other companies that provide telecommunications or related services, which may materially and adversely affect our financial condition, results of operations and growth prospects.

The telecommunications industry in China has been evolving. We, along with China Mobile Communications Corporation, or China Mobile, and China Telecommunications Corporation, or China Telecom, are the three full-service telecommunications service providers that operate both fixed-line and mobile telecommunications networks in China. See "A. History and Development of the Company — Restructurings of the Telecommunications Industry" under Item 4. We face intense competition in virtually all aspects of our services, including mobile services, fixed-line voice services, broadband services and data communications services, from China Mobile and China Telecom and expect that this competition will further intensify. In particular, we compete with China Mobile and China Telecom in mobile services. For fixed-line services, we are a leading fixed-line operator in northern China, while China Telecom has a dominant market position in southern China and the MIIT granted to China Mobile the approval for China Mobile to authorize China Mobile Limited to operate the fixed-line telecommunications business in December 2013. In addition, the PRC Government from time to time introduces new policies that may intensify competition among the three telecommunications operators. For example, the PRC government has started mobile number portability pilot programs in certain provinces and cities, and announced in March 2019 to implement the program nationwide in China by the end of 2019. The mobile number portability program allows customers to switch mobile carriers while retaining their numbers, which may intensify the competition among telecommunication operators.

Any failure or delay in expanding and upgrading our mobile networks, any increase in the associated costs (including the costs and expenses that may be incurred as a result of the changes of our marketing and sales policies) could hinder the recovery of our significant capital investment in mobile services, respectively, which could in turn have a material adverse effect on our financial condition, results of operations and growth prospects.

Our business relies on the lease arrangements with the Tower Company as to telecommunications towers and related assets, and we may not be able to achieve the expected benefits from the establishment of the Tower Company and such lease arrangements.

In July 2014, we, China Mobile and China Telecom, the three major telecommunications operators in China, jointly established the Tower Company, which engages primarily in the construction, maintenance and operation of telecommunications towers and other ancillary facilities in China, as well as the provision of maintenance services of base station equipment. In October 2015, the Tower Company acquired all telecommunications towers and related assets from us, China Mobile and China Telecom. In July 2016 and January 2018, we, through our wholly owned subsidiary, CUCL, and the Tower Company entered into a commercial pricing agreement, or the Pricing Agreement, and the supplementary agreement to such Pricing Agreement, or the Supplementary Agreement, respectively, in relation to the leasing of the telecommunications towers and related assets acquired and newly constructed by the Tower Company. In August 2018, the Tower Company completed its initial public offering and listed on the main board of the HKSE and our percentage ownership in the Tower Company decreased to 20.65% as a result. See “A. History and Development of the Company — Establishment of the Tower Company and the Disposal of Telecommunications Towers” under Item 4.

The main purpose for us to participate in the establishment of the Tower Company and lease telecommunications towers and related assets from the Tower Company is to enhance our telecommunications network coverage and capacity, realize long-term investment returns through the equity investment in the Tower Company and reduce capital expenditure as we ceased to construct telecommunications towers on our own. However, because we do not own a majority interest of, or otherwise control, the Tower Company, the Tower Company may not always act in the best interests of us, and there are uncertainties as to whether the services of the Tower Company can sufficiently support our business needs and plans, and whether the Tower Company can fulfill any usage arrangements to be agreed with us and properly operate, maintain and manage its assets.

Furthermore, since it is expected that, in principle, none of us, China Mobile or China Telecom will construct any telecommunications towers in the future, our business will rely on the lease arrangements with the Tower Company. We cannot assure you that we are able to use telecommunications towers and related assets on terms and conditions we desire. The Pricing Agreement, as supplemented and amended from time to time, provides for a pricing adjustment mechanism, which could result in a significant adjustment of the fees charged to us by the Tower Company in the future if there is any significant fluctuation in steel price, inflation and condition of the real estate market. Furthermore, prior to the expiration of lease periods of individual towers, we have to negotiate with the Tower Company new leases of such towers. If we are unable to enter into any new leases or if we are able to enter into new leases but the lease terms are less favorable to us, our business operations, financial condition and results of operations may materially and adversely affected. Failure of the Tower Company to fulfill any usage arrangements with us or properly operate, maintain and manage its telecommunications tower assets or to provide stable services to us could adversely affect the quality and uninterrupted services of our networks, which would in turn materially and adversely affect our business operations as well as our financial condition and results of operations.

We are subject to risks associated with our telecommunications equipment suppliers and other business partners which could be adversely affected by restrictions, sanctions or other legal or regulatory actions under relevant laws and regulations in various jurisdictions which in turn could adversely affect the supply chain and our business operations.

We procure our telecommunications network equipment and related maintenance and technical support from certain PRC and overseas telecommunications equipment suppliers. See "Item 4. Information on the Company—B. Business Overview—Networks." We also transact business with our business partners who may operate globally. As these parties operate globally and are therefore subject to the laws and regulations in various jurisdictions, any restrictions, sanctions or other legal or regulatory actions could cause disruptions or other material difficulties in their business activities to the extent any government of the relevant jurisdictions imposes any restrictions on their import and export activities, or sanctions or other legal or regulatory actions against the suppliers and other business partners in connection with their business activities. The relevant jurisdictions include, among others, the United States, the European Union and the United Nations. Furthermore, as the supply of our telecommunications equipment relies on a global supply chain which is vulnerable to significant disruptions in the supply of parts and other items that are necessary for the relevant manufacturing activities. Such disruptions could prevent those affected suppliers from delivering equipment and services to us in accordance with the agreed terms of supply, which in turn could negatively affect our business operations. For example, we may not be able to find suitable alternative suppliers for the affected equipment in a timely manner. Even if we are able to find alternative suppliers, the commercial terms may not be comparable, and we could therefore be subject to a higher procuring cost. Furthermore, if any of our suppliers raises their prices due to an increase in international trade tariffs, we could be subject to a higher cost in procuring the relevant products. We may experience a significant delay in implementing the part of our business plans that relies on delivery of the affected network equipment and difficulties in timely improving our services that rely on those suppliers for upgrading our networks and related software and applications. Any of these and other consequences could materially adversely affect our business, results of operations, financial condition and prospect and cause a significant volatility in and a decline in our share price.

Because we rely on arrangements with other telecommunications operators, changes to the terms or availability of these arrangements may result in disruptions to our services and operations and may result in customer dissatisfaction and materially and adversely affect our financial condition, results of operations and growth prospects.

Our ability to provide telecommunications services depends upon arrangements with other telecommunications operators. In particular, interconnection is necessary to complete all calls between our subscribers and subscribers of other telecommunications operators. We, either through ourselves or through Unicom Group, have established interconnection and transmission line leasing arrangements with other telecommunications operators, including our parent company, as required to conduct our current business. Any disruption to our interconnection with the networks of those operators or other international telecommunications operators with which we interconnect may affect our operations, service quality and customer satisfaction, thus adversely affecting our business. Furthermore, we are generally not entitled to collect indirect or consequential damages resulting from disruptions in the networks with which we are interconnected. Any disruption in existing interconnection arrangements and transmission line arrangements or any significant change of their terms, as a result of natural events or accidents or for regulatory, technical, competitive or other reasons, may lead to temporary service interruptions and increased costs that can seriously jeopardize our operations and adversely affect our financial condition, results of operations and growth prospects. Difficulties in executing alternative arrangements with other operators on a timely basis and on acceptable terms, including the inability to promptly establish additional interconnection links or increase interconnection bandwidths as required, could also materially and adversely affect our financial condition, results of operations and growth prospects.

Interruptions to our networks and operating systems or to those with which we interconnect, including those caused by natural disaster and service maintenance and upgrades, may disrupt our services and operations and may result in customer dissatisfaction and materially and adversely affect our financial condition, results of operations and growth prospects.

Our network infrastructure and the networks with which we interconnect are vulnerable to potential damages or interruptions from floods, wind, storms, fires, power loss, severed cables, acts of terrorism and similar events. The occurrence of a natural disaster or other unanticipated problems at our facilities or any other failure of our networks or systems, or the networks to which we are interconnected, may result in consequential interruptions in services across our telecommunications infrastructure. In 2018, certain areas of China suffered from natural disasters including typhoons, floods, mountain torrents, mudslides and landslides, and these natural disasters caused extensive damage to our network equipment, including our base stations and optical fiber networks, in the affected areas. As a result, we experienced service stoppage and other disruptions in our operations in those areas and also sustained economic losses. Any future natural disasters may, among other things, significantly disrupt our ability to adequately staff our business, and may generally disrupt our services and operations. Moreover, our networks and systems and the networks with which we interconnect also require regular maintenance and upgrades. Such maintenance and upgrades may cause service disruptions. Network or system failures, as well as abrupt high traffic volumes, may also affect the quality of our services and cause temporary service interruptions. Any such future occurrence may result in customer dissatisfaction and materially and adversely affect our financial condition, results of operations and growth prospects.

In addition, our operations depend on a number of services and facilities provided by Unicom Group. For example, Unicom Group provides us with international gateway services, interconnection services, sales agency and collection services and provision of premises. See "B. Related Party Transactions" under Item 7. The interests of Unicom Group as provider of these services and facilities may conflict with our interests. Failure by Unicom Group to fulfill its obligations under any of these arrangements may have a material adverse effect on our business operations. We currently have limited alternative sources of supply for these services and facilities and, as a result, may have limited ability to negotiate with Unicom Group regarding the terms for providing these services and facilities. Changes in the availability, pricing or quality of these services or facilities may have a material adverse effect on our business and profitability.

The previous internal reorganization of Unicom Group for the A Share offering created a two-step voting mechanism that requires the approval of the minority shareholders of both our Company and China United Network Communications Limited (formerly known as China United Telecommunications Corporation Limited), or the A Share Company, for significant related party transactions between us and Unicom Group.

In October 2002, Unicom Group completed an internal reorganization of its shareholding in our company and the initial public offering in China of its then newly established subsidiary, the A Share Company. As part of this restructuring, a portion of Unicom Group's indirect shareholding in our company was transferred to the A Share Company, whose business is limited to indirectly holding the equity interest of our company without any other direct business operations. A voting mechanism was established to allow public shareholders of the A Share Company to indirectly participate in our shareholders' meetings and a two-step voting mechanism was established for the approval of related party transactions. As a result, any significant related party transaction between us or our subsidiaries and Unicom Group or its other subsidiaries will require the separate approval of the independent minority shareholders of both our company and the A Share Company. Related party transactions approved by our independent minority shareholders nevertheless cannot proceed if they are not approved by the independent minority shareholders of the A Share Company. This adds another necessary step of approval process for those transactions. See "A. History and Development of the Company — Two-Step Voting Arrangements" under Item 4.

The benefits that we expect to enjoy relating to the mixed ownership reform of our ultimate controlling shareholder, Unicom Group, are subject to substantial uncertainty.

As part of the PRC government's efforts to reform state-owned enterprises and increase their competitiveness, our ultimate controlling shareholder, Unicom Group, participated in a pilot program on mixed ownership reform of state-owned enterprises, and implemented a plan to diversify its shareholders' base, or the Mixed Ownership Reform Plan, by bringing in certain strategic investors, including certain large Internet companies, into the A Share Company, our controlling shareholder. See "A. History and Development of the Company – Our Relationship with Unicom Group" and "A. History and Development of the Company — The Mixed Ownership Reform" under Item 4. The main purpose of the Mixed Ownership Reform Plan is to improve the corporate governance, incentive system and management efficiency of the A Share Company, and create synergies through cooperation with strategic investors. However, as there is substantial uncertainty with respect to our cooperation with strategic investors and the improvement in our incentive system, we cannot assure you that these benefits will be achieved as expected.

Investor confidence and the market prices of our shares and ADSs may be materially and adversely impacted if we are or our independent registered public accounting firm is unable to conclude that our internal control over financial reporting is effective in future years as required by Section 404 of the Sarbanes-Oxley Act of 2002.

We are a public company in the United States that is subject to the Sarbanes-Oxley Act of 2002. Pursuant to the requirements of Section 404 of the Sarbanes-Oxley Act of 2002, we have included in this annual report a report of management on our internal control over financial reporting and an attestation report of our independent registered public accounting firm on the effectiveness of our internal control over financial reporting.

China Netcom was incorporated in Hong Kong on October 22, 1999, under the predecessor of the Companies Ordinance as a company limited by shares under the name Target Strong Limited. The company changed its name to China Netcom (Hong Kong) Corporation Limited on December 9, 1999, to China Netcom Corporation (Hong Kong) Limited on August 4, 2000, and to China Netcom Group Corporation (Hong Kong) Limited on July 23, 2004 (the last name change in anticipation of its IPO in 2004).

As part of our integration with China Netcom, our wholly owned subsidiary, CUCL, merged with China Netcom (Group) Company Limited, or CNC China, a wholly owned subsidiary of China Netcom, in January 2009, and upon that merger becoming effective, CUCL assumed all the rights and obligations of CNC China, and all the assets, liabilities and business of CNC China were vested in CUCL. In addition, in January 2009, Unicom Group, our parent company, merged with and absorbed Netcom Group, the parent company of China Netcom. Upon completion of the merger between Unicom Group and Netcom Group, Unicom Group assumed all the rights and obligations of Netcom Group, and all the assets, liabilities and business of Netcom Group have vested in Unicom Group.

Our Relationship with Unicom Group

Our ultimate controlling shareholder is Unicom Group, a company incorporated under the laws of the PRC and majority-owned by the PRC Government. Unicom Group was established in accordance with the State Council's approval to introduce orderly competition in the telecommunications industry in 1994.

Unicom Group transferred certain of its telecommunications assets, rights and liabilities to CUCL (which became our wholly owned subsidiary in China) in April 2000 in preparation for our initial public offering, or IPO. In June 2000, we successfully completed our IPO. Our ordinary shares are listed on the HKSE and our ADSs, each representing 10 of our ordinary shares, are listed on the NYSE.

Unicom Group holds the licenses required for our telecommunications businesses and we derive our rights to operate our businesses from our status as a subsidiary of Unicom Group. Unicom Group undertook to hold and maintain all licenses received from the MIIT in connection with our businesses solely for our benefit during the term of such licenses and at no cost to us. In addition, Unicom Group undertook to take all actions necessary to obtain and maintain for our benefit such governmental licenses or approvals as we shall require to continue to operate our businesses. Unicom Group also agreed not to engage in any business which competes with our businesses other than the then-existing competing businesses of Unicom Group and to grant us a right of first refusal in relation to any government authorization, license or permit, or other business opportunity to develop any new telecommunications technology, product or service. Finally, Unicom Group also gave us an undertaking not to seek an overseas listing for any of its businesses or the businesses of its subsidiaries in which we have engaged or may engage in the future, except through us.

Set forth below is our shareholding structure as of April 16, 2019.

18. INVESTMENTS IN SUBSIDIARIES

As of December 31, 2018, the details of the Company's subsidiaries are as follows:

Name	Place and date of incorporation /establishment and nature of legal entity	Percentage of equity interests held		Particular of issued share capital/paid up capital	Principal activities and place of operation
		Direct	Indirect		
China United Network Communications Corporation Limited ("CUCL")	The PRC, April 21, 2000, limited liability company	100%	—	RMB 213,044,797,828	Telecommunications operation in the PRC
China Unicom Global Limited	Hong Kong, May 29,2015, limited company	100%	—	HKD 2,625,097,491	Investment holding
China Unicom (Hong Kong) Operations Limited	Hong Kong, May 24, 2000, limited company	—	100%	HKD 1,510,100,000	Telecommunications service in Hong Kong
China Unicom (Americas) Operations Limited	USA, May 24, 2002, limited company	—	100%	5,000 shares, USD100 each	Telecommunications service in the USA
China Unicom (Europe) Operations Limited	The United Kingdom, November 8, 2006, limited company	—	100%	4,861,000 shares, GBP1 each	Telecommunications operation in the United Kingdom
China Unicom (Japan) Operations Corporation	Japan, January 25, 2007, limited company	—	100%	1,000 shares, JPY366,000 each	Telecommunications operation in Japan
China Unicom (Singapore) Operations Pte Limited	Singapore, August 5, 2009, limited company	—	100%	30,000,000 shares, RMB1 each	Telecommunications operation in Singapore
China Unicom (South Africa) Operations (Pty) Limited	South Africa, November 19, 2012, limited liability company	—	100%	100 shares, ZAR 1 each	Telecommunications operation in South Africa
China Unicom (MYA) Operations Company Limited	The Republic of the Union of Myanmar ("Myanmar"), June 7, 2013, limited liability company	30%	70%	2,150,000 shares, USD1 each	Communications technology training in Myanmar
China Unicom (Australia) Operations Pty Limited	Australia, May 27, 2014, limited liability company	—	100%	4,350,000 shares, AUD 1 each	Telecommunications operation in Australia
China Unicom (Russia) Operations Limited Liability Company	Russia, December 28, 2016, limited liability company	—	100%	RUB10,000	Telecommunications service in Russia

Exhibit 14-M

"Nokia Corp., Nokia and China Huaxin Sign Definitive Agreements for Creation of New Nokia Shanghai Bell Joint Venture"

NOKIA

Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture

Nokia Corporation
Stock Exchange Release
May 18, 2017 at 09:00 (CET +1)

Nokia and China Huaxin sign definitive agreements for creation of new Nokia Shanghai Bell joint venture

Beijing, China - Nokia and China Huaxin Post & Telecommunication Economy Development Center ("China Huaxin") today signed the definitive agreements of the proposed integration of Alcatel-Lucent Shanghai Bell Co. Ltd. (ASB) and Nokia's China business. The new joint venture will be branded as Nokia Shanghai Bell (NSB).

As a result of today's announcement, the joint venture will become Nokia's exclusive platform in China for the continued development of new technologies in areas like IP routing, optical, fixed and next-generation 5G; and with the support of Nokia, NSB will continue to look for opportunities in select overseas markets.

ASB and Nokia's China business have been effectively operating as one entity since January 2016 when an interim operational agreement was signed.

The closing of today's agreement, targeted to happen in July 2017, is subject to various customary administrative, legal, regulatory and other conditions. Nokia will own 50% plus one share of NSB, with China Huaxin owning the remainder, and the new joint venture will have one board of directors and one management team.

NSB will represent the major part of Nokia's overall Greater China business and fully leverage both shareholders' strengths, including innovation, global scale, efficiency and a deep understanding of the local market; and with the aim of increasing Nokia's market presence in China. It will further Nokia's strategic goals of leading in high-performance networks with communication service providers and expanding to new vertical markets in enterprise, public sector, and cloud/internet companies.

NSB research and development (R&D) will be an integral part of Nokia's global R&D community, with a total of around 16 000 personnel, including 10 000 researchers, working across six R&D sites in China. It will maintain and further enhance Nokia's world-class product and research capabilities in areas that include 5G, IoT and Cloud.

NSB's R&D scope and activities will be carried out according to Nokia's applicable policies, global R&D processes and product roadmaps. NSB will also support strategic initiatives of the Chinese government and engage in long-term research projects aligned with and implementing Nokia Bell Labs' Future X Network.

Rajeev Suri, President and CEO of Nokia Corporation, said: "Today's agreement is historic for Nokia and for China, marking the next step of our decades-long commitment to the country and underscoring China's leading role in developing next-generation communication technologies. Nokia Shanghai Bell will enhance our ability to innovate, helping us strengthen ties with communication service providers and expand to new, fast-growing sectors in need of high-performing networks."

Yuan Xin, General Manager of China Huaxin, said: "We are fully confident in the new joint venture's success during the industry transformation brought by the new technologies like 5G and IoT. The successful combination globally and in China brings together the leading E2E network technologies and most powerful innovation engines from both sides. We're excited to work with Nokia to establish a future-oriented innovative technology company, with a win-win cooperative model for the bigger success in the new era."

About China Huaxin

China Huaxin Post and Telecommunication Economy Development Center is an industrial investment company that seeks long-term commercial growth opportunities in the Information and Communications Technologies (ICT) sector. China Huaxin has extensive global operations and international investment experience. China Huaxin aspires to be a competitive global industry holding group that creates long-term value for its stakeholders and for society as a whole by nurturing and advancing technology innovation in the Information Industry. www.sinohx.com

About Nokia

We create the technology to connect the world. Powered by the research and innovation of Nokia Bell Labs, we serve communications service providers, governments, large enterprises and consumers, with the industry's most complete, end-to-end portfolio of products, services and licensing. From the enabling infrastructure for 5G and the Internet of Things, to emerging applications in virtual reality and digital health, we are shaping the future of technology to transform the human experience. www.nokia.com

Media Inquiries

Nokia China Communications
LING Yi
T: +86 21 38436561
M: +86 18616388716
yi.a.ling@alcatel-sbell.com.cn

Nokia Corporate Communications
T: +358 10 448 4900
press.services@nokia.com

FORWARD-LOOKING STATEMENTS

It should be noted that Nokia and its businesses are exposed to various risks and uncertainties and certain statements herein that are not historical facts are forward-looking statements, including, without limitation, those regarding: A) our ability to integrate Alcatel Lucent into our operations and achieve the targeted business plans and benefits, including targeted synergies in relation to the acquisition of Alcatel Lucent; B) expectations, plans or benefits related to our strategies and growth management; C) expectations, plans or benefits related to future performance of our businesses; D) expectations, plans or benefits related to changes in organizational and operational structure; E) expectations regarding market developments, general economic conditions and structural changes; F) expectations and targets regarding financial performance, results, operating expenses, taxes, currency exchange rates, hedging, cost savings and competitiveness, as well as results of operations including targeted synergies and those related to market share, prices, net sales, income and margins; G) timing of the deliveries of our products and services; H) expectations and targets regarding collaboration and partnering arrangements, joint ventures or the creation of joint ventures, including the creation of the new Nokia Shanghai Bell joint venture and the related administrative, legal, regulatory and other conditions, as well as our expected customer reach; I) outcome of pending and threatened litigation, arbitration, disputes, regulatory proceedings or investigations by authorities; J) expectations regarding restructurings, investments, uses of proceeds from transactions, acquisitions and divestments and our ability to achieve the financial and operational targets set in connection with any such restructurings, investments, divestments and acquisitions; and K) statements preceded by or including "believe," "expect," "anticipate," "foresee," "sees," "target," "estimate," "designed," "aim," "plans," "intends," "focus," "continue," "project," "should," "will" or similar expressions. These statements are based on management's best assumptions and beliefs in light of the information currently available to it. Because they involve risks and uncertainties, actual results may differ materially from the results that we currently expect. Factors, including risks and uncertainties that could cause these differences include, but are not limited to: 1) our ability to execute our strategy, sustain or improve the operational and financial performance of our business and correctly identify and successfully pursue business opportunities or growth; 2) our ability to achieve the anticipated benefits, synergies, cost savings and efficiencies of the acquisition of Alcatel Lucent, and our ability to implement our organizational and operational structure efficiently; 3) general economic and market conditions and other developments in the economies where we

operate; 4) competition and our ability to effectively and profitably compete and invest in new competitive high-quality products, services, upgrades and technologies and bring them to market in a timely manner; 5) our dependence on the development of the industries in which we operate, including the cyclicality and variability of the information technology and telecommunications industries; 6) our global business and exposure to regulatory, political or other developments in various countries or regions, including emerging markets and the associated risks in relation to tax matters and exchange controls, among others; 7) our ability to manage and improve our financial and operating performance, cost savings, competitiveness and synergies after the acquisition of Alcatel Lucent; 8) our dependence on a limited number of customers and large multi-year agreements; 9) exchange rate fluctuations, as well as hedging activities; 10) Nokia Technologies' ability to protect its IPR and to maintain and establish new sources of patent licensing income and IPR-related revenues, particularly in the smartphone market; 11) our dependence on IPR technologies, including those that we have developed and those that are licensed to us, and the risk of associated IPR-related legal claims, licensing costs and restrictions on use; 12) our exposure to direct and indirect regulation, including economic or trade policies, and the reliability of our governance, internal controls and compliance processes to prevent regulatory penalties in our business or in our joint ventures; 13) our ability to identify and remediate material weaknesses in our internal control over financial reporting; 14) our reliance on third-party solutions for data storage and service distribution, which expose us to risks relating to security, regulation and cybersecurity breaches; 15) inefficiencies, breaches, malfunctions or disruptions of information technology systems; 16) Nokia Technologies' ability to generate net sales and profitability through licensing of the Nokia brand, particularly in digital media and digital health, and the development and sales of products and services, as well as other business ventures which may not materialize as planned; 17) our exposure to various legislative frameworks and jurisdictions that regulate fraud and enforce economic trade sanctions and policies, and the possibility of proceedings or investigations that result in fines, penalties or sanctions; 18) adverse developments with respect to customer financing or extended payment terms we provide to customers; 19) the potential complex tax issues, tax disputes and tax obligations we may face in various jurisdictions, including the risk of obligations to pay additional taxes; 20) our actual or anticipated performance, among other factors, which could reduce our ability to utilize deferred tax assets; 21) our ability to retain, motivate, develop and recruit appropriately skilled employees; 22) disruptions to our manufacturing, service creation, delivery, logistics and supply chain processes, and the risks related to our geographically-concentrated production sites; 23) the impact of litigation, arbitration, agreement-related disputes or product liability allegations associated with our business; 24) our ability to optimize our capital structure as planned and re-establish our investment grade credit rating or otherwise improve our credit ratings; 25) our ability to achieve targeted benefits from or successfully achieve the required administrative, legal, regulatory and other conditions and implement planned transactions, including the creation of the new Nokia Shanghai Bell joint venture, as well as the liabilities related thereto; 26) our involvement in joint ventures and jointly-managed companies; 27) the carrying amount of our goodwill may not be recoverable; 28) uncertainty related to the amount of dividends and equity return we are able to distribute to shareholders for each financial period; 29) pension costs, employee fund-related costs, and healthcare costs; and 30) risks related to undersea infrastructure, as well as the risk factors specified on pages 67 to 85 of our 2016 annual report on Form 20-F under "Operating and financial review and prospects-Risk factors" and in our other filings with the U.S. Securities and Exchange Commission. Other unknown or unpredictable factors or underlying assumptions subsequently proven to be incorrect could cause actual results to differ materially from those in the forward-looking statements. We do not undertake any obligation to publicly update or revise forward-looking statements, whether as a result of new information, future events or otherwise, except to the extent legally required.

End of the release / See all releases

Nokia press subscription

First name*

Last name*

Country*

E-mail*

Subscribe

*required information

Enquiries on this topic

Media enquiries

press.services@nokia.com

Tel. +358 10448 4900

Helsinki · Evening GMT +2 / CEST

Investor enquiries

investor.relations@nokia.com

Tel. +358 40 803 4080

Helsinki · Evening GMT +3 / EEST

Stock exchange releases

Updated: 21.05.2019 · 18:30 EEST

1 / 8

21 May 2019

Resolutions of the Nokia Annual General Meeting 2019; the Board of Directors resolved to distribute EUR 0.05 per share as the first instalment of dividend

25 Apr 2019

Nokia Corporation Interim Report for Q1 2019

18 Apr 2019

Nokia provides reca segment results an disclosures for 2018 financial reporting s

Exhibit 14-N

"Finnish Visit to Nokia Shanghai Bell"

BUSINESS NEWS, CHINA, FINLAND, TELECOMMUNICATIONS

Finnish visit to Nokia Shanghai Bell

by Joakim Persson • October 12, 2018 • 0 Comments

Facebook Twitter LinkedIn Email

Team Finland led by **Consul General Jan Wahlberg** on 10 October visited the R&D Center at **Nokia Shanghai Bell** to discuss future cooperation.

This Shanghai lab plays a unique role in building Nokia's research eco-system in China by establishing extensive cooperation between Chinese customers and top universities in China for national key projects and consortium.

Nokia Shanghai Bell is a joint venture between Nokia and China Huaxin, integrating Alcatel-Lucent Shanghai Bell Co. Ltd and Nokia's China business. The joint venture, which started its operation in July 2017, is Nokia's exclusive platform in China for the continued development of new technologies such as IP routing, optical, fixed and next-generation 5G. The facility is located in Jinqiao, east of Shanghai, and is ranked as a top 10 enterprise research center in China.

Nokia's research and development staff in China is altogether around 10 000 people in six different locations. They work as an integral part of the global Nokia R&D team.

The research team is dedicated to pioneering research in a vast array of technologies including: Wireless access and fixed access technology; 5G, advanced multiple antenna technologies; Device to device communication; Cloud RAN; Green

radio; Small cell technology; TDD specific technologies; LTE-A/beyond broadcast/multicast; Cellular based machine to machine; Software-defined converged access network; Next generation PON; and RoF-based fronthaul

Sources: Nokia Shanghai Bell, Consulate General of Finland in Shanghai

Related Posts

Finnish Minister Olli Rehn visited Shanghai

Finnish design firms in Shanghai relocated

Exhibit 14-O

"NSA Concerns Give Chinese Server Maker a Boost"

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/nsa-concerns-give-chinese-server-maker-inspur-a-boost-1406653858

TECHNOLOGY

NSA Concerns Give Chinese Server Maker a Boost

Inspur Is Taking Market Share From IBM, Other U.S. Rivals in China in Wake of Snowden Revelations

By Eva Dou

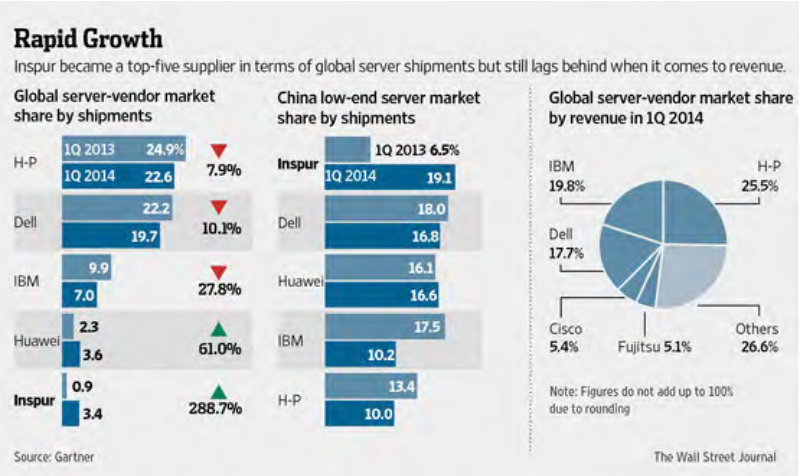
July 29, 2014 1:10 p.m. ET

BEIJING—A Chinese company that once made computer accessories is seeking to rival International Business Machines Corp. as a top provider of big-ticket computer servers in China.

Its strategy, in part: Bring up Edward Snowden.

Inspur Group Co. is using Chinese worries about U.S. gear as part of its effort to take market share from IBM, Hewlett-Packard Co. and other foreign rivals. U.S. technology companies fell under a cloud in China last year after the former U.S. National Security Agency contractor disclosed that the U.S. government was collecting sensitive data from American companies.

Inspur Chairman Sun Pishu, a member of the country's legislature, proposed measures this year to review critical technology purchases and accelerate the shift toward homegrown gear. The company unveiled a marketing program called I2I—IBM to Inspur—aimed at convincing businesses to switch from Big Blue.



Since the NSA controversy began, Inspur, which started out in the 1960s making computer accessories in China's northeast Shandong province, has seen domestic server sales soar. It overtook Dell Inc., China's Huawei Technologies Co. and H-P in the first quarter to top China's charts for server shipments, according to data from researcher Gartner.

The boom in China has also lifted Inspur to the No. 5 spot globally. U.S. vendors Dell, H-P and IBM all saw market-share declines in China and globally during the same period.

A spokesman for Dell declined to comment. Representatives at IBM and H-P didn't respond to a request for comment.

But neither Inspur nor Huawei are in the top five list globally when it comes to revenue, and even in China, they lag behind their U.S. rivals. That means foreign companies still have a firm hold on the market for the most sophisticated and expensive machines needed to run the country's big banks and other important areas, Gartner says.

RELATED

- Microsoft, the 'Guardian Warriors' and China's Cybersecurity Fears

Inspur's rapid growth showcases the successes and challenges for Beijing's long-running push to shed its dependence on the likes of IBM, Oracle Corp., Cisco Systems Inc. and other Western companies for high-tech equipment. China eventually hopes to replace Western equipment running the critical functions in major state-run banks and other government-controlled companies, though experts say that day is far off.

Beijing's push has been accelerated by rising tensions between the U.S. and China over cybersecurity threats. In recent months, major U.S. tech firms like Apple Inc. and Microsoft Corp. have been in the cross hairs of Chinese state media, which questioned the security of their technologies.

China is also pursuing antitrust investigations of both Microsoft and Qualcomm this year, showing that its officials are taking a harder line against foreign firms.

China has worked for decades to develop homegrown technologies to wean itself off its dependence on U.S. firms. Since 1986, the government has used something called the 863 Program to fund technology development in sectors deemed strategic, ranging from spacecraft to automation. Most recently, the country is pouring $5 billion into its microchip industry, as well as encouraging the development of homegrown software to compete with Microsoft's Windows and Google Inc.'s Android.

Inspur, which developed China's first pager in 1990 and first server three years later, has played a key role in the government plans. Its chairman Mr. Sun, nicknamed "the father of Chinese servers," is a member of the 863 Program's expert committee. The company worked with China's National University of Defense Technology to build the world's fastest supercomputer, China's Tianhe-2, on an 863 Program grant.

Inspur also received a 1 billion yuan ($162 million) grant under the same government program in 2009 to develop China's first high-end server. The result, Inspur's K1 Tiansuo, began sales in 2010 and remains the company's most advanced server.

Still, experts say China's server makers don't yet have the capability to make mainframes, the most advanced type of servers, and their successes are mainly due to lower prices and better device customization. "We think our customers at the end of the day make their purchase decisions based on value," said Zhang Haitao, Inspur's vice president.

An executive at one of China's biggest state-run banks said the lender's core functions run almost exclusively on foreign equipment. "It's not like cellphones," the executive said. "You can't just switch them."

IDC analyst Thomas Zhou estimates that 90% of Chinese banks' $800 million of server purchases this year will go to U.S. vendors. So far, he says, Chinese banks use locally made servers for simpler tasks such as running the software that interacts with consumers online and at kiosks.

Political factors are also driving some sales of Chinese servers, analysts say, noting that politically connected Inspur has been particularly adept at leveraging them.

"Since the end of 2012, the Chinese government has encouraged large state-owned enterprises and the government sector to buy more servers from local vendors," said Gartner analyst Uko Tian.

Shandong State-Owned Assets Investment Holdings Co. owns a controlling stake in Inspur Group. The company's server-making unit, Inspur Electronic Information Industry Co. , is publicly traded on the Shenzhen stock exchange. In March, Mr. Sun, Inspur's chairman, brought forth several proposals to the National People's Congress, where he holds a seat. One proposal was to accelerate a switch to domestically made technologies, including Inspur's K1 Tiansuo server. Another was to conduct mandatory security approvals for the suppliers of "critical information infrastructure," whose definition would be expanded to include the telecom, finance, energy and transportation industries.

In May, in the wake of U.S. charges against five Chinese military officers for spying, China's State Internet Information Office said the government would establish procedures to evaluate the security of Internet technology and services in sectors related to national security.

China's President Xi Jinping reiterated the government's commitment to developing its own technology in June, saying that science and technology were the foundation of national strength.

Unlike Inspur, Huawei has tried to shy away from the national-security issue as it tries to build out its international business—and is itself facing scrutiny in the U.S. over national-security concerns. Zheng Yelai, president of Huawei's IT product line, said in an interview he believes the company's recent sales growth in China was due to its competitive products rather than the Snowden disclosures.

Inspur's Mr. Zhang says the spying concerns have likely had some help to sales, although he wouldn't say how much.

"Customers surely have this concern," he said. "But whether they are buying because of this reason is hard to say."

—Lingling Wei contributed to this article.

Write to Eva Dou at eva.dou@wsj.com

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

Exhibit 14-P

PC Magazine's Online Product-Overview Page for Cisco Systems, Inc.'s Catalyst 3650-48P Layer 3 Switch

Cisco Catalyst 3650-48P Layer 3 Switch

$6,361.99

FREE Shipping

ADD TO CART

Product Overview

UPC Code: 882658593314
Manufacturer Warranty: Limited Lifetime
Country of Origin: CHINA

General Information

Manufacturer: Cisco Systems, Inc
Manufacturer Part Number: WS-C3650-48PS-S
Manufacturer Website Address: www.cisco.com
Brand Name: Cisco
Product Line: Catalyst
Product Series: 3650
Product Model: 3650-48P
Product Name: Catalyst 3650-48P Layer 3 Switch
Marketing Information:
The Cisco Catalyst® 3650 Series is the next generation of enterprise-class standalone and stackable access-layer switches that provide the foundation for full convergence between wired and wireless on a single platform. The Cisco Catalyst 3650 is built on the advanced Cisco StackWise®-160, and takes advantage of the new Cisco® Unified Access Data Plane (UADP) application-specific integrated circuit (ASIC). This switch can enable uniform wired-wireless policy enforcement, application visibility, flexibility, application optimization, and superior resiliency. The Cisco Catalyst 3650 Series Switches support full IEEE 802.3at Power over Ethernet Plus (PoE+), and offer modular and field-replaceable redundant fans and power supplies. They can help you increase wireless productivity and reduce your TCO.

Product Type: Layer 3 Switch

Interfaces/Ports

Total Number of Network Ports: 48
Token Ring Port: No
LRE Port: No
Uplink Port: Yes
Bypass: No
Modular: No
Management Port: Yes
Number of PoE+ (RJ-45) Ports: 48
Stack Port: Yes
Port/Expansion Slot Details: 4 x Gigabit Ethernet Uplink
Port/Expansion Slot Details: 48 x Gigabit Ethernet Network

Media & Performance

Media Type Supported: Twisted Pair
Twisted Pair Cable Standard: Category 5e
Ethernet Technology: Gigabit Ethernet
Network Technology: 10/100/1000Base-T

I/O Expansions

Number of Total Expansion Slots: 4
Expansion Slot Type: SFP
Number of SFP Slots: 4

Network & Communication

Layer Supported: 4

Management & Protocols

Manageable: Yes
Management:

- QoS
- VLAN

- Embedded Event Manager (EEM)
- RMON
- SNMP v1, 2c, 3
- MIB
- DHCP

Memory

Standard Memory: 4 GB
Memory Technology: DRAM
Flash Memory: 2 GB

Reliability

MTBF: 383760 Hour

Power Description

PoE (RJ-45) Port: No
Input Voltage: 110 V AC
Input Voltage: 220 V AC
Power Source: Power Supply
Redundant Power Supply Supported: Yes

Physical Characteristics

Compatible Rack Unit: 1U
Form Factor: Rack-mountable
Form Factor: Desktop
Height: 1.7"
Width: 17.5"
Depth: 17.6"
Weight (Approximate): 16.75 lb

Miscellaneous

System Requirements:

- Processor Speed: 233 MHz minimum
- DRAM: 512 MB
- Number of Colors: 256
- Resolution: 1024 x 768
- Font Size: Small

Operating Systems:

- Windows XP
- Windows 7
- Mac OS X

Web Browsers:

- Google Chrome
- Microsoft Internet Explorer
- Mozilla Firefox

Warranty

Limited Warranty: Lifetime

SHARE TWEET PIN IT

Related Products

Cisco Catalyst 2960X-48FPS-L Ethernet Switch

Cisco Catalyst 2960X-48LPS-L Ethernet Switc

$3,704.99 $3,144.99

← BACK TO NETWORKING

View All Categories

© 1996-2018 Ziff Davis, LLC. PCMag Digital Group
PC, PC Magazine and PC PCMag.com are among the federally registered trademarks of
Ziff Davis, LLC and may not be used by third parties without explicit permission.

Exhibit 14-Q

Excerpts from Cisco Systems, Inc.'s Form 10-K Annual Report for Fiscal Year Ended July 30, 2016

Table of Contents

UNITED STATES SECURITIES AND EXCHANGE COMMISSION

WASHINGTON, D.C. 20549

FORM 10-K

(Mark one)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the fiscal year ended July 30, 2016

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**
For the transition period from ____ to ____

Commission file number 0-18225

CISCO SYSTEMS, INC.

(Exact name of Registrant as specified in its charter)

California	**77-0059951**
(State or other jurisdiction of incorporation or organization)	**(IRS Employer Identification No.)**
170 West Tasman Drive San Jose, California	**95134-1706**
(Address of principal executive offices)	**(Zip Code)**

Registrant's telephone number, including area code: (408) 526-4000
Securities registered pursuant to Section 12(b) of the Act:

Title of Each Class:	Name of Each Exchange on which Registered
Common Stock, par value $0.001 per share	The NASDAQ Stock Market LLC

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. ☒ Yes ☐ No

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. ☐ Yes ☒ No

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. ☒ Yes ☐ No

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). ☒ Yes ☐ No

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, or a smaller reporting company. See definitions of "large accelerated filer," "accelerated filer" and "smaller reporting company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐ (Do not check if a smaller reporting company)	Smaller reporting company	☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). ☐ Yes ☒ No

Aggregate market value of registrant's common stock held by non-affiliates of the registrant, based upon the closing price of a share of the registrant's common stock on January 22, 2016 as reported by the NASDAQ Global Select Market on that date: $117,979,166,007

Number of shares of the registrant's common stock outstanding as of September 2, 2016 : 5,014,353,833

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's Proxy Statement relating to the registrant's 2016 Annual Meeting of Shareholders, to be held on December 12 , 2016, are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated.

Acquisitions

We have acquired many companies, and we expect to make future acquisitions. Mergers and acquisitions of high-technology companies are inherently risky, especially if the acquired company has yet to ship a product. No assurance can be given that our previous or future acquisitions will be successful or will not materially adversely affect our financial condition or operating results. Prior acquisitions have resulted in a wide range of outcomes, from successful introduction of new products and technologies to an inability to do so. The risks associated with acquisitions are more fully discussed in "Item 1A. Risk Factors," including the risk factor entitled "We have made and expect to continue to make acquisitions that could disrupt our operations and harm our operating results."

Investments in Privately Held Companies

We make investments in privately held companies that develop technology or provide services that are complementary to our products or that provide strategic value. The risks associated with these investments are more fully discussed in "Item 1A. Risk Factors," including the risk factor entitled "We are exposed to fluctuations in the market values of our portfolio investments and in interest rates; impairment of our investments could harm our earnings."

Strategic Alliances

We pursue strategic alliances with other companies in areas where collaboration can produce industry advancement and acceleration of new markets. The objectives and goals of a strategic alliance can include one or more of the following: technology exchange, product development, joint sales and marketing, or new market creation. Companies with which we have, or recently had, strategic alliances include the following:

Accenture Ltd; Apple Inc.; AT&T Inc.; Cap Gemini S.A.; Citrix Systems, Inc.; EMC Corporation; LM Ericsson Telephone Company; Fujitsu Limited; Inspur Group Ltd.; Intel Corporation; International Business Machines Corporation; Italtel SpA; Johnson Controls Inc.; Microsoft Corporation; NetApp, Inc.; Oracle Corporation; Red Hat, Inc.; SAP AG; Sprint Nextel Corporation; Tata Consultancy Services Ltd.; VCE Company, LLC ("VCE"); VMware, Inc.; Wipro Limited; and others.

Companies with which we have strategic alliances in some areas may be competitors in other areas, and in our view this trend may increase. The risks associated with our strategic alliances are more fully discussed in "Item 1A. Risk Factors," including the risk factor entitled "If we do not successfully manage our strategic alliances, we may not realize the expected benefits from such alliances, and we may experience increased competition or delays in product development."

Competition

We compete in the networking and communications equipment markets, providing products and services for transporting data, voice, and video traffic across intranets, extranets, and the Internet. These markets are characterized by rapid change, converging technologies, and a migration to networking and communications solutions that offer relative advantages. These market factors represent both an opportunity, and a competitive threat to us. We compete with numerous vendors in each product category. The overall number of our competitors providing niche product solutions may increase. Also, the identity and composition of competitors may change as we increase our activity in our new product markets. As we continue to expand globally, we may see new competition in different geographic regions. In particular, we have experienced price-focused competition from competitors in Asia, especially from China, and we anticipate this will continue.

Our competitors include Amazon Web Services LLC; Arista Networks, Inc.; ARRIS Group, Inc.; Avaya Inc.; Blue Jeans Networks, Brocade Communications Systems, Inc.; Check Point Software Technologies Ltd.; Citrix Systems, Inc.; Dell Inc.; Extreme Networks, Inc.; F5 Networks, Inc.; FireEye, Inc.; Fortinet, Inc.; Hewlett-Packard Enterprise Company; Huawei Technologies Co., Ltd.; International Business Machines Corporation; Juniper Networks, Inc.; Lenovo Group Limited; Microsoft Corporation; Nokia Corporation; Palo Alto Networks, Inc.; Polycom, Inc.; Riverbed Technology, Inc.; Symantec Corporation; Ubiquiti Networks and VMware, Inc.; among others.

Some of these companies compete across many of our product lines, while others are primarily focused in a specific product area. Barriers to entry are relatively low, and new ventures to create products that do or could compete with our products are regularly formed. In addition, some of our competitors may have greater resources, including technical and engineering resources, than we do. As we expand into new markets, we will face competition not only from our existing competitors but also from other competitors, including existing companies with strong technological, marketing, and sales positions in those markets. We also sometimes face competition from resellers and distributors of our products. Companies with which we have strategic alliances in some areas may be competitors in other areas, and in our view this trend may increase. For example, the enterprise data center is undergoing a fundamental transformation arising from the convergence of technologies, including computing, networking, storage, and software, that previously were segregated within the data center. Due to several factors, including the availability of highly scalable and general purpose microprocessors, application-specific integrated circuits offering advanced services, standards-based protocols, cloud computing, and virtualization, the convergence of technologies within the enterprise data center is spanning multiple,

Exhibit 14-R

Excerpts from Hewlett Packard Enterprise Co.'s Form 10-K Annual Report for Fiscal Year Ended Oct. 31, 2018

Table of Contents

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended October 31, 2018
Or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission file number 001-37483

HEWLETT PACKARD ENTERPRISE COMPANY

(Exact name of registrant as specified in its charter)

Delaware	**47-3298624**
(State or other jurisdiction of incorporation or organization)	(I.R.S. employer identification no.)
3000 Hanover Street, Palo Alto, California	**94304**
(Address of principal executive offices)	(Zip code)

Registrant's telephone number, including area code: **(650) 687-5817**
Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Common stock, par value $0.01 per share	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act:
None

Indicate by check mark if the registrant is a well-known seasoned issuer as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer", "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act. (Check one):

Large accelerated filer ☒	Accelerated filer ☐	Non-accelerated filer ☐ (Do not check if a smaller reporting company)	Smaller reporting company ☐
			Emerging growth company ☐

HPE StoreOnce and HPE Recovery Manager Central, solutions for secondary workloads and traditional tape, storage networking and disk products, such as HPE MSA and HPE XP.

- *DC Networking.* Our offerings include top-of-rack switches, core switches, and open networking switches. We offer a full stack of networking solutions that deliver open, scalable, secure and agile solutions, by enabling programmable fabric, network virtualization, and network management products.

- HPE Pointnext creates preferred IT experiences that power the digital business. The HPE Pointnext team and our extensive partner network provide value across the IT life cycle delivering advice, transformation projects, professional services, support services and operational services for Hybrid IT and the Intelligent Edge. HPE Pointnext is also a provider of on-premises flexible consumption models, such as HPE GreenLake, that enable IT agility, simplify operations and align cost to business value. HPE Pointnext offerings includes Operational Services, Advisory and Professional Services, and Communication and Media Solutions ("CMS").

Intelligent Edge

The Intelligent Edge business is comprised of enterprise networking and security solutions for businesses of any size, offering secure connectivity for campus and branch environments, operating under the Aruba brand. The primary business drivers for Intelligent Edge solutions are mobility and IoT.

- *HPE Aruba Product* includes wired and wireless local area network hardware products such as Wi-Fi access points, switches, routers, sensors, and software products that include network management, network access control, analytics and assurance, and location services software .
- *HPE Aruba Services* offers professional and support services for the Intelligent Edge portfolio of products.

Financial Services

Financial Services provides flexible investment solutions, such as leasing, financing, IT consumption, and utility programs and asset management services, for customers that facilitate unique technology deployment models and the acquisition of complete IT solutions, including hardware, software and services from Hewlett Packard Enterprise and others. In order to provide flexible services and capabilities that support the entire IT life cycle, FS partners with customers globally to help build investment strategies that enhance their business agility and support their business transformation. FS offers a wide selection of investment solution capabilities for large enterprise customers and channel partners, along with an array of financial options to SMBs and educational and governmental entities.

Corporate Investments

Corporate Investments includes Hewlett Packard Labs and certain business incubation projects.

Our Strengths

We believe that we possess a number of competitive advantages that distinguish us from our competitors, including:

Strong solutions portfolio for the data center, cloud and intelligent edge . We combine our software-defined infrastructure and services capabilities to provide what we believe is the strongest portfolio of enterprise solutions in the IT industry. Our ability to deliver a comprehensive IT strategy-from the cloud to the data center to the intelligent edge, through our high-quality products and high-value consulting and support services in a single package-is one of our principal differentiators.

Multi-year innovation roadmap . We have been in the technology and innovation business for over 75 years. Our vast intellectual property portfolio and global research and development capabilities are part of a broader innovation roadmap designed to help organizations take advantage of the expanding amount of data available and leverage the latest technology developments like cloud, artificial intelligence, and cybersecurity to drive business outcomes now and in the future.

Global distribution and partner ecosystem . We are experts in delivering innovative technological solutions to our customers in complex multi-country, multi-vendor and/or multi-language environments. We have one of the largest go-to-market capabilities in our industry, including a large ecosystem of channel partners, which enables us to market and deliver our product offerings to customers located virtually anywhere in the world.

Custom financial solutions . We have developed innovative financing solutions and IT consumption models to facilitate the delivery of our products and services to our customers. We deliver flexible investment solutions and expertise that help customers and other partners create unique technology deployments based on specific business needs.

costs and expenses, and require substantial expenditures and recovery time in order to fully resume operations. Our corporate headquarters and a portion of our research and development activities are located in California, which has suffered from drought conditions and catastrophic wildfires affecting the health and safety of our employees. Other critical business operations and some of our suppliers are located in California and Asia, near major earthquake faults known for seismic activity. In addition, our principal worldwide IT data centers are located in the southern United States, making our operations more vulnerable to climate-related natural disasters, such as 2017 hurricane Harvey, which caused severe damage in Houston. The manufacture of product components, the final assembly of our products and other critical operations are concentrated in certain geographic locations, including the Czech Republic, Mexico, China and Singapore. We also rely on major logistics hubs, primarily in Asia to manufacture and distribute our products, and primarily in the southwestern United States to import products into the Americas region. Our operations could be adversely affected if manufacturing, logistics or other operations in these locations are disrupted for any reason, including natural disasters, IT system failures, military actions or economic, business, labor, environmental, public health, regulatory or political issues. The ultimate impact on us, our significant suppliers and our general infrastructure of being located near vulnerable locations is continuing to be assessed .

Our uneven sales cycle makes planning and inventory management difficult and future financial results less predictable.

In some of our businesses, our quarterly sales have periodically reflected a pattern in which a disproportionate percentage of each quarter's total sales occurs towards the end of the quarter. This uneven sales pattern makes predicting revenue, earnings, cash flow from operations and working capital for each financial period difficult, increases the risk of unanticipated variations in our quarterly results and financial condition and places pressure on our inventory management and logistics systems. If predicted demand is substantially greater than orders, there may be excess inventory. Alternatively, if orders substantially exceed predicted demand, we may not be able to fulfill all of the orders received in each quarter and such orders may be canceled. Depending on when they occur in a quarter, developments such as a systems failure, component pricing movements, component shortages or global logistics disruptions, could adversely impact our inventory levels and results of operations in a manner that is disproportionate to the number of days in the quarter affected.

We experience some seasonal trends in the sale of our products that also may produce variations in our quarterly results and financial condition. For example, sales to governments (particularly sales to the U.S. government) are often stronger in the third calendar quarter, and many customers whose fiscal year is the calendar year spend their remaining capital budget authorizations in the fourth calendar quarter prior to new budget constraints in the first calendar quarter of the following year. European sales are often weaker during the summer months. Typically, our third fiscal quarter is our weakest and our fourth fiscal quarter is our strongest. Many of the factors that create and affect seasonal trends are beyond our control.

Changes in U.S. trade policy, including the imposition of tariffs and the resulting consequences, may have a material adverse impact on our business and results of operations.

The U.S. government has adopted a new approach to trade policy and in some cases to renegotiate, or potentially terminate, certain existing bilateral or multi-lateral trade agreements. It has also imposed tariffs on certain foreign goods, including information and communication technology products. These measures may materially increase costs for goods imported into the United States. This in turn could require us to materially increase prices to our customers which may reduce demand, or, if we are unable to increase prices, result in lowering our margin on products sold. Changes in U.S. Trade policy have resulted in, and could result in more, U.S. trading partners adopting responsive trade policy making it more difficult or costly for us to export our products to those countries.

Any failure by us to identify, manage and complete acquisitions, divestitures and other significant transactions successfully could harm our financial results, business and prospects.

As part of our business strategy, we may acquire companies or businesses, divest businesses or assets, enter into strategic alliances and joint ventures and make investments to further our business (collectively, "business combination and investment transactions"). For example, in April 2017, we acquired Nimble Storage, Inc., which provides predictive all-flash and hybrid-flash storage solutions. In May 2016, we completed the sale to Tsinghua Holdings Co., Ltd. ("Tsinghua"), the asset management arm of Tsinghua University in China, of a 51% interest in our wholly owned subsidiary that owns and operates H3C Technologies and our China-based server, storage and technology services businesses for approximately $2.6 billion. On April 1, 2017 and September 1, 2017, we spun off our Enterprise Services and Software businesses, respectively. See also the risk factors below under the heading “Risks Related to the Separations of our Former Enterprise Services Business and our Former Software Segment”.

Risks associated with business combination and investment transactions include the following, any of which could adversely affect our revenue, gross margin, profitability and financial results:

ITEM 1B. Unresolved Staff Comments.

None.

ITEM 2. Properties.

As of October 31, 2018 , we owned or leased approximately 18 million square feet of space worldwide. A summary of the Company's operationally utilized space is provided below.

	As of October 31, 2018		
	Owned	Leased	Total
	(Square feet in millions)		
Administration and support	4.3	6.9	11.2
(Percentage)	38%	62%	100%
Core data centers, manufacturing plants, research and development facilities, and warehouse operations	1.0	1.4	2.4
(Percentage)	42%	58%	100%
Total	5.3	8.3	13.6
(Percentage)	39%	61%	100%

We believe that our existing properties are in good condition and are suitable for the conduct of our business. Substantially all of our properties are utilized in whole or in part by our Hybrid IT and Intelligent Edge segments.

In connection with the HPE Next initiative, we continue to anticipate changes in our real estate portfolio over the next two years. These changes may include reductions in overall space, and an increase in leased space as a percentage of total space.

Principal Executive Offices

Our principal executive offices, including our global headquarters, are located at 3000 Hanover Street, Palo Alto, California, 94304, United States of America ("U.S."). Our principal executive offices, including our global headquarters is expected to be relocated to a facility at 6280 America Center Drive, San Jose, California, 95002, U.S. and this move is expected to be completed by early fiscal 2019.

Product Development, Services and Manufacturing

The locations of our major product development, manufacturing, and Hewlett Packard Labs facilities are as follows:

Americas

Brazil— Campinas
Puerto Rico —Aguadilla

United States —Alpharetta, Andover, Austin, Carrollton, Chippewa Falls, Colorado Springs, Fremont, Fort Collins, Houston, Milpitas, Palo Alto, Roseville, San Jose, Santa Clara, Sunnyvale

Europe, Middle East, Africa

United Kingdom —Bristol, Erskine

Asia Pacific

China —Beijing, Shanghai
India —Bangalore
Japan —Tokyo
Singapore— Singapore
Taiwan— Taipei

ITEM 3. Legal Proceedings.

Information with respect to this item may be found in Note 18, "Litigation and Contingencies", to the Consolidated Financial Statements in Item 8 of Part II, which is incorporated herein by reference.

full potential and derive business insights. Key solutions include HPE 3PAR Storage and HPE Nimble Storage all-flash arrays for mission critical workloads and general purpose workloads, respectively, and big data solutions running on HPE Apollo Servers. Storage also provides comprehensive data protection with HPE StoreOnce and HPE Recovery Manager Central, solutions for secondary workloads and traditional tape, storage networking and disk products, such as HPE MSA and HPE XP.

  - *DC Networking* offerings include top-of-rack switches, core switches, and open networking switches. The Company offers a full stack of networking solutions that deliver open, scalable, secure and agile solutions, by enabling programmable fabric, network virtualization, and network management products.

- HPE Pointnext creates preferred IT experiences that power the digital business. The HPE Pointnext team and the Company's extensive partner network provide value across the IT life cycle delivering advice, transformation projects, professional services, support services and operational services for Hybrid IT and the Intelligent Edge. HPE Pointnext is also a provider of on-premises flexible consumption models, such as HPE GreenLake, that enable IT agility, simplify operations and align cost to business value. HPE Pointnext offerings includes Operational services, Advisory and Professional Services, and Communication and Media Solutions ("CMS").

The *Intelligent Edge* business is comprised of enterprise networking and security solutions for businesses of any size, offering secure connectivity for campus and branch environments, operating under the Aruba brand. The primary business drivers for Intelligent Edge solutions are mobility and the Internet of Things ("IoT").

  - *HPE Aruba Product* includes wired and wireless local area network hardware products such as Wi-Fi access points, switches, routers, sensors, and software products that include network management, network access control, analytics and assurance, and location services software .
  - *HPE Aruba Services* offers professional and support services for the Intelligent Edge portfolio of products.

Financial Services provides flexible investment solutions, such as leasing, financing, IT consumption, and utility programs and asset management services, for customers that facilitate unique technology deployment models and the acquisition of complete IT solutions, including hardware, software and services from Hewlett Packard Enterprise and others. In order to provide flexible services and capabilities that support the entire IT life cycle, FS partners with customers globally to help build investment strategies that enhance their business agility and support their business transformation. FS offers a wide selection of investment solution capabilities for large enterprise customers and channel partners, along with an array of financial options to SMBs and educational and governmental entities.

Corporate Investments includes Hewlett Packard Labs and certain business incubation projects.

Segment Policy

Hewlett Packard Enterprise derives the results of its business segments directly from its internal management reporting system. The accounting policies that Hewlett Packard Enterprise uses to derive segment results are substantially the same as those the consolidated company uses. The CODM measures the performance of each segment based on several metrics, including earnings from operations. The CODM uses these results, in part, to evaluate the performance of, and to allocate resources to each of the segments.

Segment revenue includes revenues from sales to external customers and intersegment revenues that reflect transactions between the segments on an arm's-length basis. Intersegment revenues primarily consist of sales of hardware and software that are sourced internally and, in the majority of the cases, are financed as operating leases by FS to our customers. Hewlett Packard Enterprise's consolidated net revenue is derived and reported after the elimination of intersegment revenues from such arrangements.

Hewlett Packard Enterprise periodically engages in intercompany advanced royalty payment and licensing arrangements that may result in advance payments between subsidiaries. Revenues from these intercompany arrangements are deferred and recognized as earned over the term of the arrangement by the Hewlett Packard Enterprise legal entities involved in such transactions; however, these advanced payments are eliminated from revenues as reported by Hewlett Packard Enterprise and its business segments. As disclosed in Note 8, "Taxes on Earnings", Hewlett Packard Enterprise executed intercompany advanced royalty payment arrangements resulting in advanced payments of $63 million and $439 million during fiscal 2018 and 2017, respectively. In these transactions, the payments were received in the U.S. from a foreign consolidated affiliate, with a deferral of intercompany revenues over the term of the arrangements. The impact of these intercompany arrangements is eliminated from both Hewlett Packard Enterprise's consolidated and segment net revenues.

Exhibit 14-S

"Magic Quadrant for LTE Network Infrastructure"

Magic Quadrant for LTE Network Infrastructure

Published: 25 July 2016 ID: G00277823

Analyst(s): Kosei Takiishi, Jessica Ekholm, Sylvain Fabre, Frank Marsala, Peter Liu

Summary

Long Term Evolution rollouts continue as more than 500 network-based CSPs have rolled out commercial 4G LTE service. Gartner compares the 10 vendors of end-to-end (radio access and core) infrastructure for LTE networks to help CSP CTOs find the right one for their needs.

Market Definition/Description

This Magic Quadrant evaluates vendors of "end-to-end" Long Term Evolution (LTE) infrastructure — the term Gartner uses to denote radio and core network of cellular infrastructure — for communications service providers (CSPs) wanting to deploy LTE technology, whether as an overlay or with partial integration with, and some reuse of, existing network equipment (see Note 1).

The market for LTE network infrastructure products for CSPs is maturing. Products considered in this Magic Quadrant include radio access infrastructure (eNodeBs and small cells) located in base station sites, and core network equipment, which is where switching and radio resource management are handled. The core network equipment for LTE, a 4G technology, includes new elements not found in 2G and 3G networks, such as the Mobility Management Entity, a packet data network gateway and a serving gateway. This report also considers the IP Multimedia Subsystem (IMS) infrastructure and network elements required for the provision of voice over LTE (VoLTE), which are located in the core network. Also considered from last year are the vendors' approaches for LTE network alternative use cases, such as machine-to-machine (M2M).

We forecast that the worldwide market for end-to-end LTE network infrastructure will grow from $20.9 billion in 2016 to $36.6 billion in 2020, to account for 70% of spending on mobile network infrastructure (see "Forecast: Communications Service Provider Operational Technology, Worldwide, 2013-2020, 1Q16 Update"). We expect LTE to remain the fastest-growing segment of the mobile network infrastructure market.

The worldwide market for end-to-end LTE network infrastructure includes 10 vendors that provide both radio access and core network elements for LTE (see Figure 1).

Magic Quadrant

Figure 1. Magic Quadrant for LTE Network Infrastructure

Research image courtesy of Gartner, Inc.

Source: Gartner (July 2016)

Vendor Strengths and Cautions

Cisco

Cisco is a dominant player in the Evolved Packet Core (EPC) segment of LTE, including policy control, and a supplier of centralized self-organizing networks (SONs). Cisco does not have macrocell/microcell products, but the partnership with Ericsson announced in November 2015 could make amends for that. Incremental revenue opportunities of $1 billion or more are expected for each company by 2018, but in terms of the LTE radio access network, Cisco's returns would be small. Regarding LTE small cells, Cisco is leveraging its enterprise channels to market for reselling SpiderCloud Wireless radio products (with, for example, agreements with Vodafone).

STRENGTHS

Cisco is a leader in the EPC segment, and its Virtualized Packet Core also receives major CSPs' interest. It is a leader in Internet Protocol (IP) technology, which is an advantage as EPC is an all-IP network technology.

Of the vendors in this Magic Quadrant, Cisco has one of the highest scores for overall financial viability.

In 2016, Cisco announced to buy Jasper Technologies, which provides an Internet of Things (IoT) platform. This IoT service has a broad geographic reach, and its integration with existing IoT products can push forward Cisco's Internet of Everything (IoE)/IoT vision of collaborating with other ecosystem partners.

CAUTIONS

The perception among some CSPs is that Cisco still remains principally an IT player.

The vision of the partnership between Ericsson and Cisco to create the networks of the future is interesting, but so far, its progress resulting from the alliance is primarily limited to IP networks and solutions.

Cisco's IMS for VoLTE solution relies on partners, and some CSPs have indicated this can increase project management overhead.

Datang Telecom

Datang Telecom Technology & Industry Group manufactures radio and core network equipment with a focus on Time Division-Synchronous Code Division Multiple Access (TD-SCDMA) and Time Division-Long Term Evolution (TD-LTE) segments. It is best-known for its leading role in developing the Chinese TD-SCDMA 3G mobile telecommunications standard.

In the LTE segment, Datang mobile focuses on TD-LTE and the Chinese market. The company offers end-to-end solutions for TD-LTE networks, including core, access and test terminals. It is one of the TD-LTE suppliers selected by all three Chinese operators, and the company continues seeking out international TD-LTE opportunities, especially in emerging markets, such as Africa and Eastern Europe.

STRENGTHS

Datang is an early adopter and specialist in time division duplex (TDD)-related technologies (TD-SCDMA, TD-LTE and TD-LTE-Advanced) for which it holds a large set of patents.

Datang is a state-owned company and has been positioned as a TDD technology pilot. The support from government in both policy and finance allows Datang to continuously invest in LTE-related research and development.

Datang still has a relatively big market share in the TD-SCDMA market, which it can leverage to sell its TD-LTE solutions with upgrading concepts. Its TD-LTE products have been selected by all three Chinese CSPs' TD-LTE networks, albeit in a minor role.

CAUTIONS

Datang lacks visibility in the global LTE infrastructure market and is involved only in TD-LTE, a minor variety of LTE infrastructure.

Datang lacks system integration and deployment experience in LTE, which is one of the key barriers to wider adoption by CSPs.

In addition to Datang's brand being little-known outside China, the company's focus on TDD technology in its home market does not help it increase its visibility abroad, as the bulk of LTE deployments use frequency division duplex (FDD).

Ericsson

Ericsson remains in a strong position globally in the LTE infrastructure market. The company's end-to-end LTE and multistandard offerings for core, radio access network (RAN), IMS/VoLTE and software-defined networking (SDN)/network function virtualization (NFV), and its installed base in wireless CSPs' networks, together with its professional services, put it in a strong position to win business from CSPs. Ericsson is aggressively cooperating with leading CSPs on the next-generation technology (5G) and seems to be in a strong position to establish a continuous relationship with them. Nevertheless, Ericsson faces continued challenges from competitors, and several CSPs perceive it as lacking flexibility, such as regarding features, pricing structure and support.

STRENGTHS

Ericsson has long had a strong focus on mobile networks, and it is one of the leaders in terms of numbers of LTE deals. Ericsson has many 2G, 3G and 4G accounts in all geographies, including the United States — a country in which some of its competitors are less strong or have yet to enter the LTE market. Incumbency in 2G and 3G accounts has proved invaluable for any vendor looking to supply LTE upgrades, and Ericsson's many long-standing relationships with CSPs are a solid advantage in terms of making it one of the "go to" vendors for LTE upgrades.

CSPs' feedback indicated that the hardware quality and software stability of Ericsson's products are excellent, and the company's customers were first to commercially launch 600 Mbps service using Category 11 devices (using FDD LTE) and have tested the world's first commercial deployments of three-carrier TDD-and-FDD carrier aggregation with 256 quadrature amplitude modulation (QAM).

Ericsson is active with ecosystem partners addressing multiple verticals, such as public safety, utilities and connected cars. Ericsson promotes cellular for IoT with NB-IoT and LTE Category M, and its M2M/IoT connectivity platform — the Device Connection Platform (DCP) — is very useful for CSPs to support IoT/M2M devices.

CAUTIONS

While Ericsson's overall financial position is good, the company's recent growth and profitability have been challenged by a difficult macro environment. The company has announced structural changes to address these concerns, which may include layoffs and further cost cuts in the near term. Such changes must be monitored given their potential for disruption.

Several CSPs have noted that Ericsson can lack flexibility — for example, with most CSPs having to align to Ericsson's features, roadmap and delivery priorities, rather than the other way around.

Ericsson and Cisco formed a global business and technology partnership in November 2015. Their vision to create the networks of the future is interesting, but since Ericsson is relatively self-sufficient in terms of products and services, so far its progress from the alliance is primarily limited to IP networks and solutions.

FiberHome

FiberHome Technologies is one of the leading telecommunications equipment providers with a focus on optical communications. It is best-known for supplying the first optical fiber deployment in China and its leading position in China's optical fibers and cables and optical access network market.

FiberHome has been producing cellular radio products since 1997 and has been shipping small cells since 2014. Other than transmission and access, FiberHome also has core network products but is relatively weak compared with other vendors. Its TD-LTE products were in the suppliers' list of all three CSPs in China. To date, it has been awarded a small portion of the China TD-LTE market share, and its activities have been limited in its home market, China.

STRENGTHS

FiberHome is a state-owned company, and its relationship with the government can help it to continue to gain some market share in China's TD-LTE, especially in its base — Hubei Province.

FiberHome's leading position in the Chinese optical fiber market and close relationships with domestic CSPs can be leveraged for further expansion of its local TD-LTE business.

CAUTIONS

FiberHome focuses on TD-LTE technology and plays a relatively minor role, even in the Chinese LTE market. It has a limited product portfolio and a lack of visibility in the global LTE market.

The revenue from TD-LTE is a very small portion of FiberHome's total revenue, which has limited its investment in LTE 5G-related product development, such as the IoT, multiple input/multiple output (MIMO) and SDN/NFV.

Fujitsu

Fujitsu is a Japanese ICT vendor focused on the technology solution business that includes the IoT, cloud, big data and mobile. Fujitsu has a broad portfolio of IT services, but its mobile network infrastructure business is very focused on the Japanese market, and has only LTE commercial agreements with Japanese CSPs. It cooperates with Nokia on the development of Serving GW (S-GW) and Packet Data Network GW (P-GW) on the EPC provided to NTT Docomo.

STRENGTHS

Fujitsu offers the BroadOne LTE eNodeB base station family with a distributed architecture consisting of a remote radio head and a baseband unit and LTE femtocell for indoor/outdoor use and for enterprises. The BroadOne femtocell supports multifrequency bands, and selects automatically the operating frequency depending on actual network. Fujitsu's Femtocell GW can manage and operate data and control signals to reduce the high load on the core network.

A significant share of NTT Docomo's early investment in LTE in Japan went to Fujitsu, and KDDI also started to use its LTE femtocell that can support VoLTE. Thanks to the relationship with leading CSPs, Fujitsu can improve its product quality quickly.

Fujitsu provides not only mobile network infrastructure but also devices, including smartphones, tablets and feature phones. This can help to improve the quality of its mobile infrastructure product.

CAUTIONS

Fujitsu is very Japan-centric; its only two customers for LTE network infrastructure are in Japan. We have seen no evidence of traction or new contracts in international markets.

Fujitsu's LTE infrastructure product portfolio is not as comprehensive as that of the Leaders.

Huawei

Huawei holds a strong position globally in the LTE market, despite having its sales potential limited by political concerns in the United States, Australia and other countries. The company has a comprehensive portfolio, and its common radio access architecture has been widely accepted by CSPs. Huawei's MBB 2020 Strategy is composed of progressive enhancements of cellular technologies culminating in the future 5G standard. The strategy focuses on supporting more 4G subscribers, more video traffic and the IoT. The company has improved its professional and managed service capability with its SmartCare service solution.

STRENGTHS

Huawei has heavy R&D investment for both FDD and TDD technologies, and it is known to work hard to satisfy customers' demands. Huawei is involved in major TD-LTE network deployments in China, Japan and Europe. It has developed a TD-LTE-based trunking system for use in industries other than telecommunications, which could represent a business opportunity for CSPs.

Huawei has a comprehensive product portfolio not limited to LTE, which includes servers, storage, routers and switches. Optical transportation gives the company an advantage in addressing today's convergence and "cloudification" requirements.

Feedback from CSPs shows that Huawei's portfolio offers more scale and breadth than those in many more-specialized competitors, with a roadmap and feature support that are more aggressive than some competitors'.

CAUTIONS

Political resistance in the United States, Australia and other countries to granting Huawei unencumbered market access continues to prevent the company from gaining 4G network share in markets where CSPs would like to buy from it.

The vendor lock-in of competitors' existing Global System for Mobile Communications (GSM), Universal Mobile Telecommunications System (UMTS) and FDD LTE customers is still challenging, especially in advanced countries.

Huawei has grown organically in the telecommunications industry and is inclined to try to do everything by itself. On the other hand, it has become more active in the partnership and collaboration with various stakeholders during the past few years, but to be a leader in the IoT/5G era, Huawei still needs to improve its partnership strategy further and become more open.

NEC

NEC was one of the first vendors to articulate the need for smaller cells in LTE networks — long before this became a marketing trend. It has international aspirations for LTE networks and has won reference customers outside Japan. NEC is also an early adopter to support SDN/NFV on the CSP network infrastructure, and its virtualized Evolved Packet Core (vEPC) solution has been commercialized.

STRENGTHS

NEC has the capability not only as a mobile network equipment vendor to CSPs but also as a system integrator for M2M/IoT applications for users such as enterprises and the public sector. Their internal collaboration can create values such as value-added service (VAS) integration in the small-cell solution and mobile-edge computing (MEC) introduction.

NEC has a solid customer base in its home market in Japan. It supplied its technology — for example, LTE RAN and core network elements — to NTT Docomo. It has good support for advanced features, such as carrier aggregation, Cloud RAN and SDN/NFV.

NEC's microwave radio system "Pasolink" contributes to reliable, high-capacity backhaul for LTE, and it provides an advantage in supporting Cloud RAN architecture that is fundamental for LTE-Advanced (LTE-A) and 5G in the future.

CAUTIONS

NEC has made some progress toward achieving its ambitions for a global LTE presence, but its commercial deals are still limited because of insufficient marketing, brand invisibility, very Japan-centric product management and shortage of local support. CSPs should confirm its country-level support carefully.

NEC's LTE product portfolio is not as wide as those of the Leaders, making it harder to avoid commoditization.

Japanese radio frequency allocation for LTE is quite different from global trends, so NEC needs to refine its RAN offering to overcome vendor lock-in situations in its global business.

Nokia

Nokia is a leader in the LTE mobile network infrastructure market. It had transformed itself into a lean wireless network specialist but completed its acquisition of Alcatel-Lucent in January 2016. Nokia's presence in deployed LTE networks has enabled it to establish a business for its LTE-A solution and also contribute to testing advanced products, such as its AirScale, which is capable of supporting 5G. On the other hand, Nokia must continue to demonstrate that it can maintain its financial discipline and strong execution as it rationalizes and integrates the assets and operations of Alcatel-Lucent.

STRENGTHS

Nokia has a comprehensive, end-to-end LTE solution that includes radio, EPC, SON, voice core network, transport, network management, security products, public safety and professional services.

As a combined entity, the new Nokia now comes first among the leading vendors in terms of the number of LTE contracts signed.

Nokia has strong traction in countries including Brazil, Russia, India, China, Japan and South Korea for wireless network infrastructure, and it benefits from having good 3G and 4G presence and skills. The new Nokia now also benefits from a strong North American presence brought by Alcatel-Lucent's footprint.

CAUTIONS

Nokia is undertaking a complex integration with Alcatel-Lucent that includes eliminating portfolio overlap and reducing overlapping personnel. Although the current management team's track record in making such changes has been good, there is potential for disruption due to these changes, and therefore, they must be monitored.

Feedback from CSPs shows that Nokia's product portfolio and technology roadmap were slightly less aggressive compared with other Leaders.

CSP clients of the previous Alcatel-Lucent and Nokia need to care about existing products' continuity, including hardware maintenance and software updates and migration plans.

Samsung

Samsung is a South Korean network equipment vendor and is a relatively late comer to the business of Third Generation Partnership Project (3GPP)-based cellular technology. Samsung is also an early innovator of new cellular technologies, such as vEPC, small cell and Cloud RAN.

STRENGTHS

Samsung has established a position in large-scale LTE deployments in South Korea, North America and Japan. It also penetrated the Middle East in 2011 and European LTE markets in 2012, after establishing Samsung Networks Europe.

Samsung has participated in some very advanced commercial deployments of technology (including LTE-A and Cloud RAN solutions) with South Korean CSPs, which are the world's most advanced mobile network operators, and has also conducted some early 5G-related demonstrations. The company is focusing extensively on small-cell technologies and products supporting LTE in the unlicensed spectrum. Its aim is to make LTE-Unlicensed (LTE-U)-enabled small cells to be commercially available in 2016.

Samsung is one of the leading smartphone vendors, and the internal collaboration can help to improve its product quality and push forward its business.

CAUTIONS

Samsung's lack of presence in the 2G/3G network infrastructure market globally hampers its ability to expand its share of the LTE network infrastructure market, as CSPs tend to favor incumbent vendors for upgrades. It is observed that Samsung didn't announce many new LTE customer additions by 1Q16.

Despite some good international traction for its LTE base station business, Samsung's core network business has not yet extended in the global market.

Samsung is very aggressive in cooperating with CSPs around 5G testing, but its momentum is not as strong as three Leaders: Ericsson, Huawei and Nokia.

ZTE

ZTE is one of the key players in the LTE mobile infrastructure market. It places strong emphasis on China and other Asia/Pacific markets, and it has made some progress toward becoming a bigger international player, with some good reference cases, such as MTN. The experience that the company gained from LTE projects in China helps it break through into some key new markets, such as Southeast Asia, India and Europe. ZTE recently unveiled its Pre5G initiatives, which include both early commercialization of 5G key technologies and LTE-Advanced Pro and will build the bridge connecting 4G and 5G.

STRENGTHS

ZTE is a leading supplier in the Chinese 3G/4G market and a key player in the global mobile infrastructure market. This provides it with a steady stream of revenue and much network-building experience.

ZTE continues to demonstrate, test and interoperate advanced capabilities with CSPs — for example, massive MIMO and cloud radio — in order to gain mind share and market share. It has become increasingly visible in Asia (for example, in SoftBank's LTE network in Japan and Telkomsel's LTE in Indonesia), Europe, the Middle East, Africa and Latin America. It can also use its fixed-line products and relationships in these markets to help it access CSPs wanting LTE upgrades and to deepen its cooperation with them.

Feedback from CSPs includes praise for ZTE's flexibility and responsiveness specifically during the initial rollout phase. Its recently improved marketing communications could help it gain visibility.

CAUTIONS

Although ZTE is branching out from China as it gains more contracts and a wider footprint in international markets, it still needs to boost its presence and mind share in more countries. ZTE could benefit from hiring more local support engineers with local network knowledge and language skills as it becomes more international.

ZTE still experiences difficulty competing against stronger players for Tier 1 CSP accounts in Western Europe, in addition to political resistance in some countries. The election of the new board of directors and leadership members in April 2016 also resulted from some security challenges. In the future, it needs to focus on compliance much more and improve its global business.

ZTE is aggressively seeking to have a 5G partnership with CSPs, but its momentum is not as strong as the other three Leaders: Ericsson, Huawei and Nokia.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we

have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

FiberHome Technologies

Dropped

Alcatel-Lucent, after the acquisition by Nokia

Inclusion and Exclusion Criteria

Vendors in this Magic Quadrant supply end-to-end LTE network infrastructure equipment to network-based CSPs. End-to-end equipment includes radio access and core network elements.

Products considered in this Magic Quadrant include radio access infrastructure (eNodeBs and small cells), located in base station sites, and core network equipment, which is where switching and radio resource management are handled. The core network equipment for LTE, a 4G technology, includes new elements not found in 2G and 3G networks, such as the Evolved Packet Core (EPC), which includes the Mobility Management Entity, a packet data network gateway and a signaling gateway. This report also considers the IP Multimedia Subsystem (IMS) infrastructure and network elements required for the provision of voice over LTE (VoLTE), which are located in the core network. This year, we also consider the vendors' approaches for LTE network alternative use cases, such as M2M.

Several vendors have made progress in their security, as well as NFV offerings around LTE, and while these capabilities will get more attention over time from CSPs, they have not yet appeared as a critical, deciding factor in LTE infrastructure procurement and vendor management decisions.

All of the vendors featured have reference customers for LTE technology with CSPs. Many are also covered elsewhere in Gartner's mobile network infrastructure research.

Evaluation Criteria

Ability to Execute

Gartner evaluates technology vendors on the quality and efficacy of the processes, systems, methods and procedures that enable their performance to be competitive, efficient and effective, and to benefit revenue, retention and reputation. Ultimately, we judge vendors on their ability to capitalize on their vision and their success in doing so.

The vendors' positions on the Ability to Execute axis were determined by evaluating them against the following criteria:

Product/Service. Goods and services offered by the vendor that compete in the defined market (radio and core network elements for LTE carrier infrastructure, as well as 4G small cells and IMS support). This includes current product and service capabilities, quality, feature sets and skills, whether offered natively or through OEM agreements or partnerships, as defined in the Market Definition/Description section and detailed in subcriteria. Both radio (macro and small cells) and core network equipment (EPC and IMS) are included. Professional services offerings, including system integration skills specifically relating to LTE, are also considered. In addition, potential advantages gained in the LTE market through capabilities in important neighboring segments are taken into account.

Overall Viability (Business Unit, Financial, Strategy and Organization). This criterion includes an assessment of the overall organization's financial health, which underpins the financial and practical success of the relevant LTE business unit, and the likelihood of that business unit continuing to invest in the product, offer the product and advance the state of the art within the organization's portfolio.

Market Responsiveness and Track Record. The vendor's ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customers' needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness, as well as market traction demonstrated through LTE contract wins. In addition, it covers the vendor's ability to adapt and scale activities to work with its own partners as well as crucial third parties (such as regulators, municipalities and civil works contractors) — in other words, to "cast a wide net" while still being able to execute and scale quickly when opportunities turn into actual LTE contracts.

Marketing Execution. The clarity, quality, creativity and efficacy of programs designed to deliver the vendor's message in order to influence the market, promote the vendor's brand and business, increase awareness of its products, and establish a positive identification with its products, brand and organization in the minds of buyers. This mind share can be driven by a combination of publicity, promotion, thought leadership, word of mouth and sales activities. Also considered is the vendor's

ability to market solutions in different regulatory contexts and to adapt to different CSPs' LTE business models.

Customer Experience. Relationships, products, services and programs that enable the vendor's clients to succeed with the products evaluated. Specifically, this includes the ways in which customers receive technical support or account support. It can also include ancillary tools, customer support programs (and the quality thereof), the availability of user groups, and SLAs.

Table 1. Ability to Execute Evaluation Criteria

Evaluation Criteria

Weighting

Product/Service

High

Overall Viability

Medium

Sales Execution/Pricing

No Rating

Market Responsiveness/Track Record

High

Marketing Execution

Medium

Customer Experience

Medium

Operations

No Rating

Source: Gartner (July 2016)

Completeness of Vision

Gartner also evaluates technology vendors on their ability to articulate logical statements about the market's current and future direction, innovation, customer needs, and competitive forces, and on how well these statements correspond to Gartner's position. Ultimately, vendors are rated on their understanding of how market forces can be exploited to create opportunities for CSPs.

We determined the vendors' positions on the Completeness of Vision axis by evaluating them against the following criteria:

Market Understanding. The vendor's ability to understand buyers' needs and to translate them into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance them with their added vision. The ability to see LTE in the wider context of CSPs' overall network transformation strategies is particularly important, though this insight must be reflected directly in the vendor's product roadmap.

Marketing Strategy. We look for a clear, differentiated set of messages, consistently communicated throughout the organization and externalized through a website, advertising, customer programs and positioning statements. We also assess the alignment of the vendor's LTE marketing strategy and its overall LTE portfolio strategy, including regional focus.

Offering (Product) Strategy. A vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature set as they map to current and future requirements. This includes differentiated approaches to the different LTE segments, including traditional carriers, municipalities and utilities.

Vertical Strategy. The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including verticals.

Innovation. Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes. This includes:

Sustained evidence of technological expertise and adoption of latest advanced features

Ability to commit to an individual CSP's network rollout, where economically feasible

New product development milestones and compliance with the roadmap of milestones

Migration path for existing wireless network infrastructure technologies, including upgrade evolution to LTE, LTE-Advanced, LTE-Advanced Pro and 5G

Support for ecosystem partners via interfaces and interoperability

Demonstration of appropriate budget for R&D planning

Geographic Strategy. The vendor's strategy to direct resources, skills and offerings to meet the specific needs of its home markets — typically outside its native geography — either directly or through partners, channels and subsidiaries, as appropriate for those geographies and markets.

Table 2. Completeness of Vision Evaluation Criteria

Evaluation Criteria

Weighting

Market Understanding

High

Marketing Strategy

Medium

Sales Strategy

No Rating

Offering (Product) Strategy

Medium

Business Model

No Rating

Vertical Strategy

High

Innovation

High

Geographic Strategy

Medium

Source: Gartner (July 2016)

Quadrant Descriptions

Leaders

Leaders typically have a significant number of commercial references for the LTE network equipment market. They also have momentum in this area, as exemplified by new contract wins. They have a broad portfolio and, even where they need partners, they are the preferred prime vendors for CSPs. They appear in nearly all CSP procurements and trials of LTE infrastructure as de facto suppliers, and their presence in the Leaders quadrant tends to be fairly stable. These are high-viability technology providers. They are well-positioned with their current product portfolios and likely to continue to deliver leading products. Leaders do not necessarily offer the best solution for every customer requirement, however, and their products may not be "best of breed" in every area. Overall, Leaders provide solutions that offer relatively low risk and can achieve and sustain deployments of high quality.

Challengers

Challengers have strong market execution capabilities and good solutions, but overall their products lack the breadth and depth of those of Leaders. Their solutions do not indicate a clear vision for how the market is evolving and are not as innovative or advanced as those of Leaders.

Visionaries

Visionaries demonstrate a clear understanding of the market and provide key innovative elements that are illustrative of the market's future. They lack the ability to influence a large part of the market, or have not yet fully expanded their sales and support capabilities to achieve global reach, or do not yet have the funding and scale to execute with the capabilities of Leaders. A characteristic of Visionaries is that their positions in the Magic Quadrant may potentially move over time into other quadrants, where they could attain a more stable state. They could, for example, achieve this stability by gaining strength and scale or wider market adoption (presence in multiple geographical markets and recognition), in which case they could enter the Leaders quadrant, or by judiciously specializing in a smaller segment and ceasing activities in others as part of a strategic transformation, in which case they could enter the Niche Players quadrant.

Niche Players

Niche Players tend to offer products that focus on a particular segment of the market (for example, a given country, such as Japan) or a subset of functionality (such as TD-LTE). They also tend to be more specialized with regard to regional coverage and/or technology. This can be an advantage, because CSPs aligned with the focus of Niche Players can find these vendors' offerings very suitable. In some cases, Niche Players have made specific decisions about where and where not to compete, so being a Niche Player does not preclude having a well-defined strategy. They could also prove attractive partners for some of the larger vendors in this market, thanks to their market specialisms or technological strengths.

Context

When shortlisting vendors, CSPs should take into account the many commitments they need to make when deploying LTE infrastructure in terms of capital investment in eNodeBs for radio access, core network elements and backhaul, as well as time, project duration and the impact on network complexity when LTE is added as an overlay. LTE deployments are such complex projects that replacing an underperforming vendor after implementation has begun can be impractical, even if liquidated damages and penalties are included in the terms of the contract.

There are multiple LTE vendors for CSPs to choose from, but they vary greatly in the scale and scope of their offerings. It is, therefore, vital that CSPs look for equipment providers that have a clear and differentiated network value proposition and strategy, and that emphasize their differentiation, functionality and features. They should also expect quality software.

CSPs also need to know that their vendor will maintain an adequate roadmap and enable them to sustain a high-performance network. Vendors therefore need to show evidence of resources, expertise and capital for investment in LTE technology in the longer term. With regard to vendors

seeking business outside their home market, CSPs should look for evidence that these vendors have effective strategies to direct resources to meet the specific needs of their intended international markets.

To gauge how well vendors meet the above requirements, Gartner scores them using a series of criteria that we developed to capture their capabilities when it comes to addressing CSPs' wants and needs for end-to-end LTE infrastructure, as described above. These criteria are summed up in our framework as vendors' Ability to Execute and Completeness of Vision.

Several vendors in the lower half of the Magic Quadrant (Cisco, Fujitsu, NEC and Samsung) are much broader and larger technology conglomerates than those in the top half. The Leaders in the top half therefore naturally have more commitment to this segment, as they expect to generate a significant proportion of their overall revenue from it. This has strategic implications for vendor selection because, for CSPs, LTE is bound to require a long-sales-cycle, long-cost-recovery model, as well as an upgrade path to 5G networks.

Market Overview

As of 2 June 2016, 503 LTE networks in 167 countries have been commercially launched, according to GSA. Most of them deployed LTE using the FDD mode only, but almost 50 CSPs deployed LTE using the TDD mode only, and almost 20 operators deployed using both LTE FDD and TDD modes.

End-user uptake of LTE will depend on several factors, such as the availability of affordable LTE service plans and LTE-enabled devices. The availability and price of LTE-enabled devices will play a key role in LTE uptake. We forecast that by the end of 2016, LTE devices will reach a $75 price point, which will give the LTE market a boost in terms of reaching end-user segments that have so far shied away from LTE services due to the high price of LTE devices. We predict that, by the end of 2020, sales of FDD LTE and TD-LTE mobile phones to end users will reach 1,683,846,000, which is 81.8% of all sales to end users (see "Forecast: Mobile Phones, Worldwide, 2013-2020, 1Q16 Update").

In terms of service pricing, an increasingly competitive market will create downward pressure on service prices, and we predict that during this year, the price difference between a 3G and an LTE service will be less than 3%. A growing number of CSPs will not be charging a premium for LTE access. Revenue potential lies in being able to offer a superior network experience and thus increase brand recognition and retention and prevent churn. Additionally, we expect an LTE user to use more data than a 3G user; thus, there are upsell opportunities for CSPs.

The growth in LTE users is helping boost mobile data traffic, as the enhanced network experience has encouraged more users to use data-hungry apps such as streaming video. In our latest consumer mobile app survey, we asked, "How long at a time do you typically stream video using your provider's cellular network?" We found that 29% streamed 30 minutes or more, and that the average streaming time per session was 19.1 minutes. In addition, we found that 85% of the U.S. respondents used YouTube regularly and 68% watched Netflix regularly on their mobile phones.

Thus the increased availability of LTE networks, with the launch of new service plans offering more bandwidth at a lesser price, as well as the improved integration of video into mobile apps by 2018, will contribute to the tripling of consumption of mobile video by early adopters from 15 minutes per day.

In terms of usage per LTE connection, we expect that a 4G smartphone user will use 5.3GB of data per month in 2018 and in comparison, a 3G smartphone user will use 1.4GB of data per month (see "Forecast: Mobile Data Traffic, Worldwide, 2011-2018" for further information). Thus, by 2018, a 4G smartphone user will use 3.7 times more data per month than a 3G smartphone user. In total, despite only 17% of all mobile connections utilizing 4G networks, we estimate that 46% of all mobile traffic will be generated by 4G connections by 2018.

This Magic Quadrant examines vendors of end-to-end (radio and core) LTE network infrastructure, but Gartner also monitors several vendors that do not yet meet the minimum criteria for inclusion because they do not offer end-to-end LTE network equipment, instead focusing on only the radio network or the core network. For example, Potevio, New Postcom Equipment and Mitsubishi Electric offer only radio products; Brocade announced its first virtualized Evolved Packet Core (vEPC) offering in 2016.

The number of large vendors in the end-to-end LTE network infrastructure market could continue to decline, as happened in the 2G/3G market even before the latest economic downturn. Further consolidation remains possible, because there are still many vendors in the mobile network infrastructure market, some of which face financial problems or lack the scale and reach needed to remain relevant. CSPs should, therefore, generally continue to consider a diverse set of stable vendors to minimize the risk of disruption from acquisitions in, or departures from, this market, while containing supplier management overheads — although some CSPs have chosen to use a single vendor for their entire mobile network. As network complexity increases with multiband, multilayer (2G, 3G, 4G and Wi-Fi, and soon 5G) and heterogeneous networks with macro and small cells, and now carrier aggregation, it becomes increasingly attractive to use a single vendor just to ensure quality of service and accountability.

In the latest large acquisition in this segment, Nokia gained control of Alcatel-Lucent through a successful public exchange offer in January 2016. Ericsson and Cisco announced a global business and technology partnership to create the networks of the future in November 2015. Vendor alliances and consolidations aim to increase economies of scale and operational efficiency and improve financial standing; however, technology evolution could happen increasingly fast, with new disruptive technologies, such as SDN/NFV, which could allow alternative vendors, such as HP and Intel to come into the LTE infrastructure market.

The race to win business in the LTE infrastructure market is far from over, and vendors are achieving different degrees of traction when it comes to securing commercial contracts with CSPs. CSPs evaluating vendors for selection should consider whether they have a history of high-quality delivery. They should also favor vendors with a strong track record that effectively promotes their LTE network equipment brand and provides clear differentiation beyond standards. CSPs should partner with vendors that show vision and understand their wants and needs. They should choose a vendor not just for its "boxes," but also for long-term service and support, and ultimately also as a partner to help them with their business models for LTE and succeeding technologies.

Most CSPs plan to integrate small cells into their LTE architecture. The more mature LTE networks are already using small cells in their networks, and the number of small cells is increasing rapidly. Small cells are used in a variety of situations: to increase capacity at busy outdoor locations, to provide coverage and capacity at large indoor locations, to provide services within large, medium and small enterprises, to provide femtocell coverage within households and branch offices, and to provide coverage to rural communities and remote locations. Different situations require a different mix of equipment attributes from LTE equipment vendors, and a specific deployment scenario might favor a given vendor over others; but feedback from CSPs is that even with the Leaders, different markets and deployment scenarios dictate using more than one vendor's 4G RAN.

Evidence

Questionnaires sent to and completed by vendors provided Gartner with an up-to-date view of their activities and achievements in relation to LTE.

We held direct discussions with technical personnel from CSPs that have deployed LTE infrastructure from one or more of the vendors profiled.

We also conducted surveys investigating all available and relevant commercial contracts for LTE involving the vendors concerned.

Local Gartner analysts provided country- and region-specific views, as appropriate.

We also requested that vendors provide supplementary information to use in our research.

Our analysis also reflects earlier briefings and credible sources, including publicly available information.

Note 1

Long Term Evolution

"LTE" was initially intended as an acronym to identify the new radio access network introduced in Release 8 of the 3GPP's standards. Its application has since been extended to the entire technology, including core network elements. In this Magic Quadrant, LTE includes not only LTE of 3GPP Release 8 but also LTE-Advanced of 3GPP Release 10 and LTE-Advanced Pro of 3GPP Release 13.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."

Exhibit 14-T

Excerpts from Lenovo Group Ltd.'s 2017/18 Annual Report

Lenovo Group Limited | 2017/18 Annual Report

Stock Code 992

Lenovo™

ABOUT LENOVO

Lenovo (HKSE: 992) (ADR: LNVGY) is a US$45 billion Fortune 500 company with a vision to become the global leader in Intelligent Transformation through smart devices and infrastructure that create the best user experience. Lenovo manufactures one of the world's widest portfolio of connected products, including smartphones (Motorola), tablets, PCs (Thinkpad, Yoga, Lenovo Legion) and workstations as well as AR/VR devices and smart home/office solutions. Lenovo's next generation data center solutions (ThinkSystem, ThinkAgile) are creating the capacity and computing power for the connections that are changing business and society. Lenovo works to inspire the different in everyone and build a smarter future where everyone thrives. Follow us on LinkedIn, Facebook, Twitter, Instagram, Weibo, or visit us at http://www.lenovo.com.

Other non-operating expenses (net) for the years ended March 31, 2018 and 2017 comprise:

For the year ended March 31	2018 US$'000	2017 US$'000
Finance income	**32,145**	27,795
Finance costs	**(263,160)**	(231,627)
Share of (losses)/profits of associates and joint ventures	**(2,506)**	21,411
	(233,521)	(182,421)

Finance income mainly represents interest on bank deposits.

Finance costs for the year increased by 14 percent as compared with last year. This is mainly attributable to the interest expense of US$20 million in relation to the 5-Year US$500 million notes, issued in March 2017, bearing annual interest at 3.875%, and the increase in factoring cost of US$43 million, partly offset by the decrease in interest on promissory note issued to Google Inc. of US$41 million.

Share of (losses)/profits of associates and joint ventures represents operating (losses)/profits arising from principal business activities of respective associates and joint ventures.

FINANCIAL POSITION

The Group's major balance sheet items are set out below:

Non-current assets	2018 US$'000	2017 US$'000
Property, plant and equipment	**1,304,751**	1,236,250
Prepaid lease payments	**507,628**	473,090
Construction-in-progress	**382,845**	413,160
Intangible assets	**8,514,504**	8,349,145
Interests in associates and joint ventures	**35,666**	32,567
Deferred income tax assets	**1,530,623**	1,435,256
Available-for-sale financial assets	**373,077**	255,898
Other non-current assets	**181,759**	122,221
	12,830,853	12,317,587

37 PRINCIPAL SUBSIDIARIES *(continued)*

Company name	Place of incorporation/ establishment	Issued and fully paid up capital	Percentage of issued capital held 2018	2017	Principal activities
Lenovo Tecnologia (Brasil) Ltda	Brazil	BRL4,424,321,818	**100%**	100%	Manufacturing and distribution of IT products
Lenovo (Thailand) Limited	Thailand	THB243,000,000	**100%**	100%	Distribution of IT products as well as mobile phone, smart phone and tablet, server and storage
Lenovo (United States) Inc.	United States	US$1	**100%**	100%	Distribution of IT products
Lenovo (Venezuela), SA	Venezuela	VEB3,846,897	**100%**	100%	Distribution of IT products
聯想（西安）有限公司 (Lenovo (Xian) Limited)[1] (Chinese-foreign equity joint venture)	Chinese Mainland	RMB10,000,000	**100%**	100%	Provision of IT services and distribution of IT products
LLC "Lenovo (East Europe/Asia)"	Russia	RUB1,910,000	**100%**	100%	Distribution and marketing of IT products
Medion AG	Germany	EUR48,418,400	**79.83%**	79.83%	Retail and service business for consumer electronic products
Motorola Mobility Comércio de Produtos Eletronicos Ltda.	Brazil	BRL756,663,401	**100%**	100%	Developer, owner, licensor and seller of communications hardware and software
Motorola Mobility International Sales LLC	United States	-	**100%**	100%	Holding company

37 PRINCIPAL SUBSIDIARIES *(continued)*

Company name	Place of incorporation/ establishment	Issued and fully paid up capital	Percentage of issued capital held 2018	2017	Principal activities
Motorola Mobility LLC	United States	-	**100%**	100%	Developer, owner, licensor and seller of communications hardware and software
NEC Personal Computers, Ltd.	Japan	JPY500,000,000	**66.64%**	66.64%	Manufacturing and distribution of IT products
深圳聯想海外控股有限公司 (Shenzhen Lenovo Overseas Holdings Limited)[1] (wholly-foreign owned enterprise)	Chinese Mainland	US$760,822,799.24	**100%**	100%	Investment management
Stoneware, Inc.	United States	US$861,341.25	**100%**	100%	Development and distribution of IT products
陽光雨露信息技術服務（北京）有限公司 (Sunny Information Technology Service, Inc.)[1] (Chinese-foreign equity joint venture)	Chinese Mainland	RMB50,000,000	**100%**	100%	Provision of repair services for computer hardware and software systems

Notes:

(i) All the above subsidiaries operate principally in their respective places of incorporation or establishment.

(ii) All the Chinese Mainland subsidiaries and Motorola's subsidiaries are limited liability companies. They have adopted December 31 as their financial year end date for statutory reporting purposes. For the preparation of the consolidated financial statements, financial statements of these Chinese Mainland subsidiaries and Motorola's subsidiaries for the years ended March 31, 2017 and 2018 have been used.

(iii) Medion AG is a publicly traded German stock corporation listed on the Frankfurt am Main stock exchange. The percentage of issued capital held is equivalent to approximately 86.51% (2017: 86.51%) excluding treasury shares.

(iv) In November 2017, the Company entered into an equity interest transfer and framework agreement in relation to disposal of 100% equity interest in 聯想移動通信軟件（武漢）有限公司 (Lenovo Mobile Communication Software (Wuhan) Limited) to a third party.

(v) The company whose English name ends with a "1" is a direct transliteration of its Chinese registered name.

Exhibit 14-U

"USA Smartphone Market Share: By Quarter"

US Smartphone Market Share: By Quarter

FEBRUARY 19, 2019 | IN DATA | BY TEAM COUNTERPOINT

Data on this page is updated every quarter

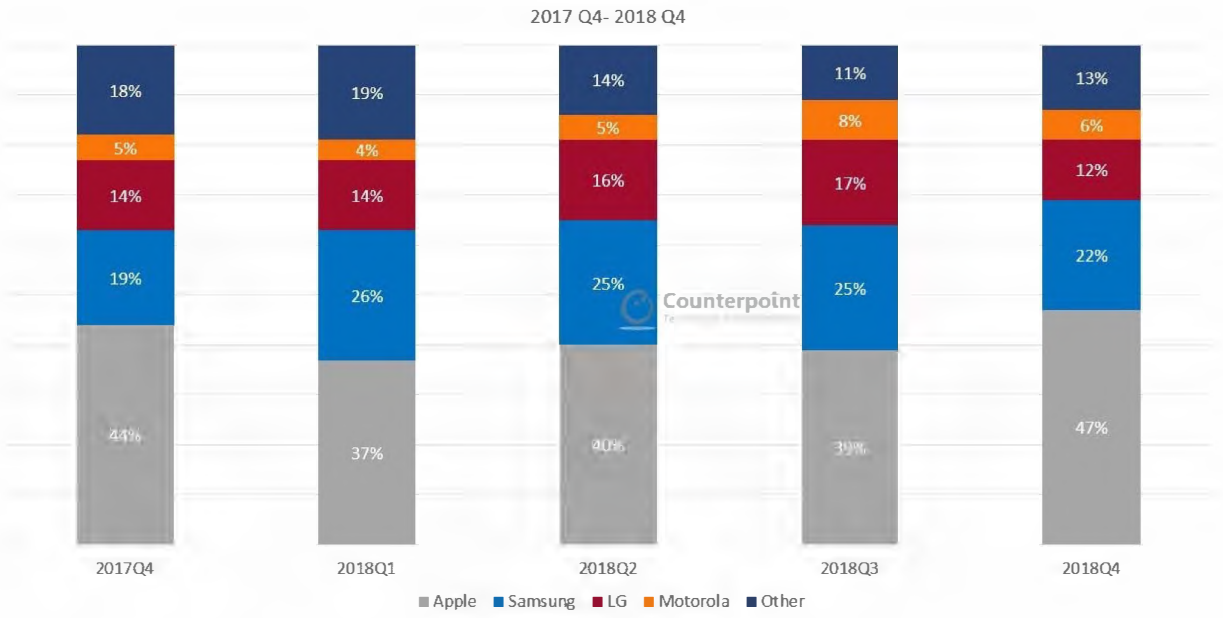
This data represents the US smartphone market share by quarter (from 2016-2018) by top OEMs. The US smartphone market is mainly an operator-driven market.

For detailed insights on the data, please reach out to us at **info(at)counterpointresearch.com**. If you are a member of the press, please contact us at **press(at)counterpointresearch.com** for any media enquiries.

Q4 2018 Highlights

- The US market sold-through 10% fewer smartphones in the fourth quarter of 2018 than the same quarter in 2017.
- Apple: Early adopters hit the stores in September and October to purchase the XS Max and XS. In November and December, the largest volumes moved to the XR.
- Verizon was the largest channel for Apple in 4Q18.
- The only gainers during 4Q18 were Alcatel, Motorola, and Samsung. Alcatel and Motorola grew from small bases.
- Samsung was able to gain on the longevity of the Galaxy S9 and S9 Plus and a particularly strong November for

the Note 9. J7 and J3 variants are strong within many prepaid channels.

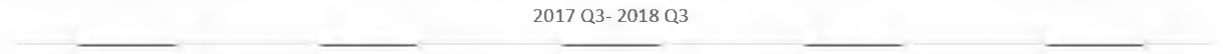


US Smartphone Shipments Market Share (%)	2017Q4	2018Q1	2018Q2	2018Q3	2018Q4
Apple	**44%**	**37%**	**40%**	**39%**	**47%**
Samsung	**19%**	**26%**	**25%**	**25%**	**22%**
LG	**14%**	**14%**	**16%**	**17%**	**12%**
Motorola	**5%**	**4%**	**5%**	**8%**	**6%**
Other	**18%**	**19%**	**14%**	**11%**	**13%**

Ranking is according to latest quarter.

Q3 2018 Highlights

- The USA smartphone market showed an annual decline of 7%.
- Apple is still leading the US Smartphone market with a 39% share in Q3 2018.
- Motorola showed a YoY growth of 54% in Q3 2018.
- Top four brands contributed to about 90% of the total market share.

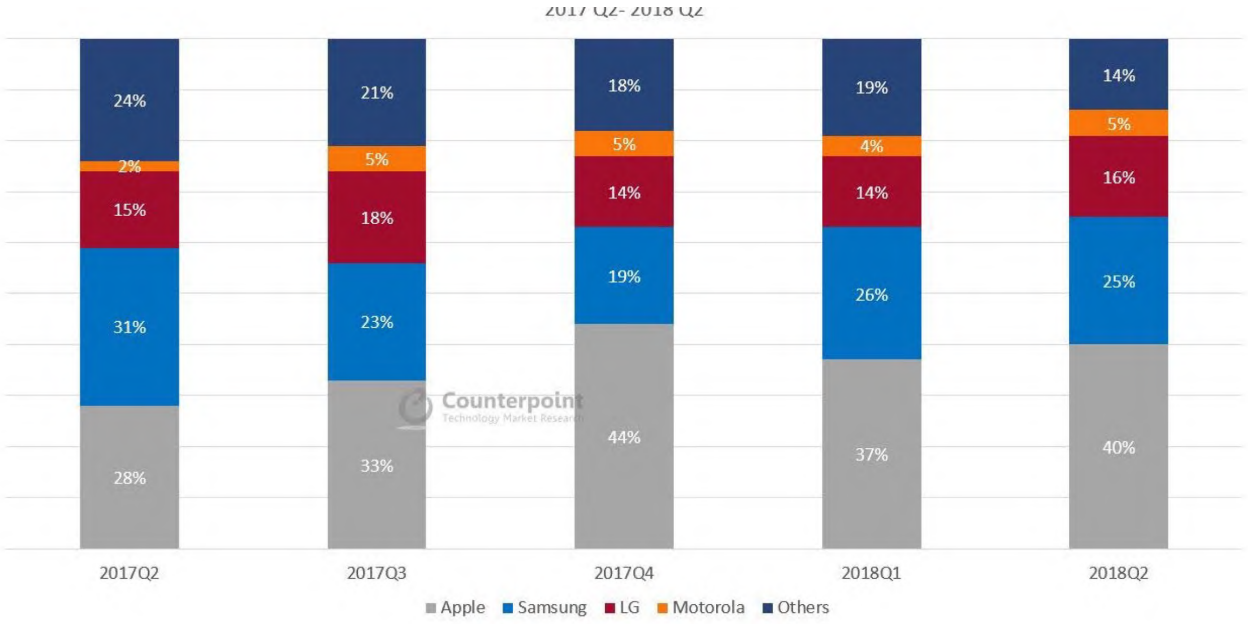


US Smartphone Shipments Market Share (%)	2017Q3	2017Q4	2018Q1	2018Q2	2018Q3
Apple	**33%**	**44%**	**37%**	**40%**	**39%**
Samsung	**23%**	**19%**	**26%**	**25%**	**25%**
LG	**18%**	**14%**	**14%**	**16%**	**17%**
Motorola	**5%**	**5%**	**4%**	**5%**	**8%**
Others	**21%**	**18%**	**19%**	**14%**	**11%**

Ranking is according to latest quarter.

Q2 2018 Highlights

- The US smartphone market declined 22% annually in Q2 2018.
- The decline in the smartphone market was majorly due to ZTE and Samsung. ZTE was affected due to sanctions imposed by the US government.
- Even though device sales were down by double digits, US wireless performances were solid in Q2 2018.

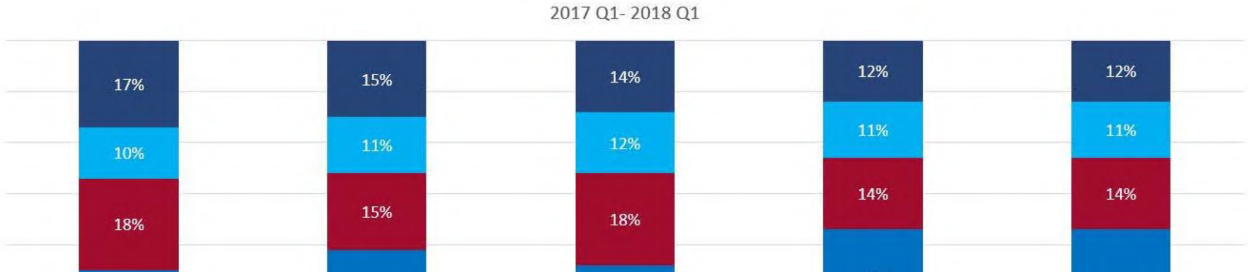


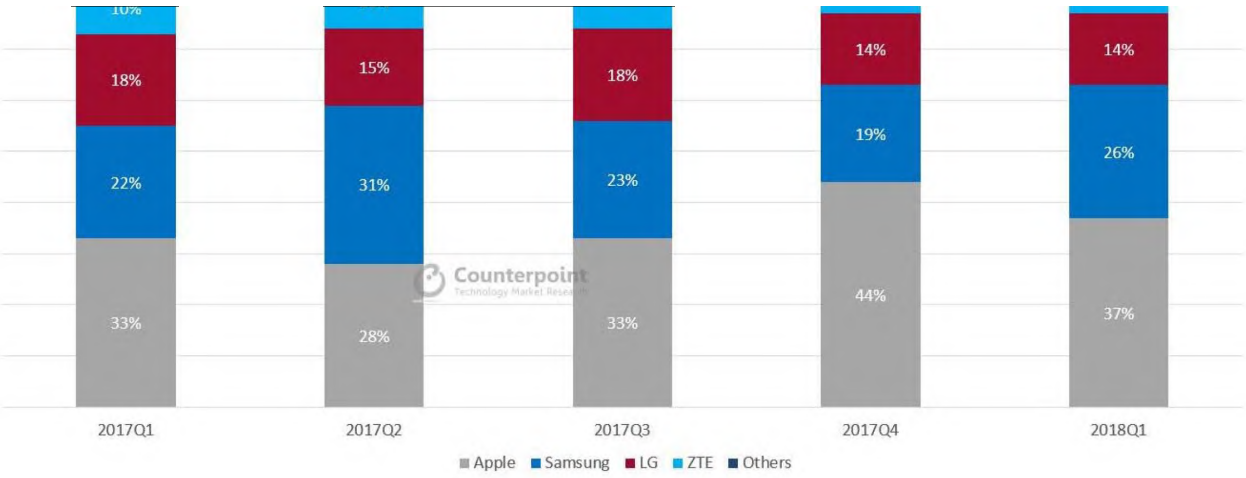
US Smartphone Shipments Market Share (%)	2017Q2	2017Q3	2017Q4	2018Q1	2018Q2
Apple	**28%**	**33%**	**44%**	**37%**	**40%**
Samsung	**31%**	**23%**	**19%**	**26%**	**25%**
LG	**15%**	**18%**	**14%**	**14%**	**16%**
Motorola	**2%**	**5%**	**5%**	**4%**	**5%**
Others	**24%**	**21%**	**18%**	**19%**	**14%**

Ranking is according to latest quarter.

Q1 2018 Highlights

- The US smartphone market declined by 1% in Q1 2018 compared to Q1 2017
- Apple continued to dominate the smartphone market with 38% share and grew annually because the iPhone X performed well in the market
- LG declined annually due to a shift in its flagship smartphone launch strategy



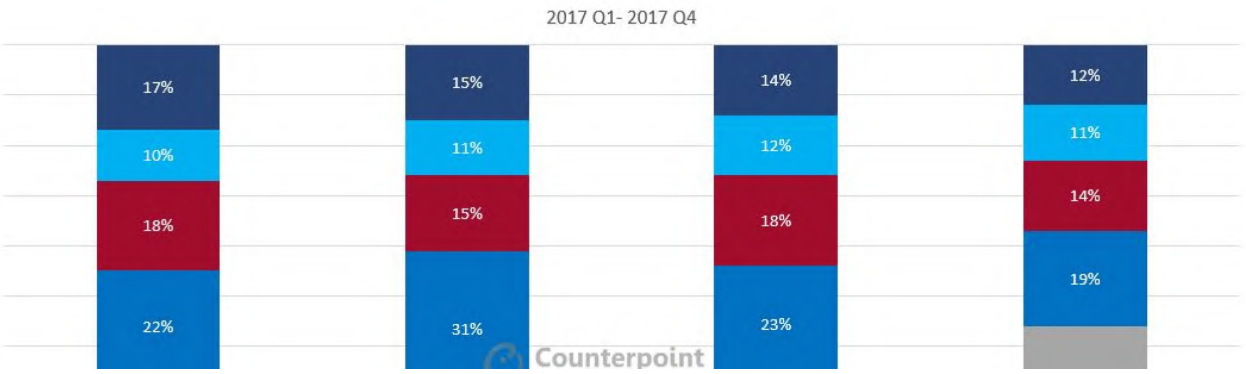


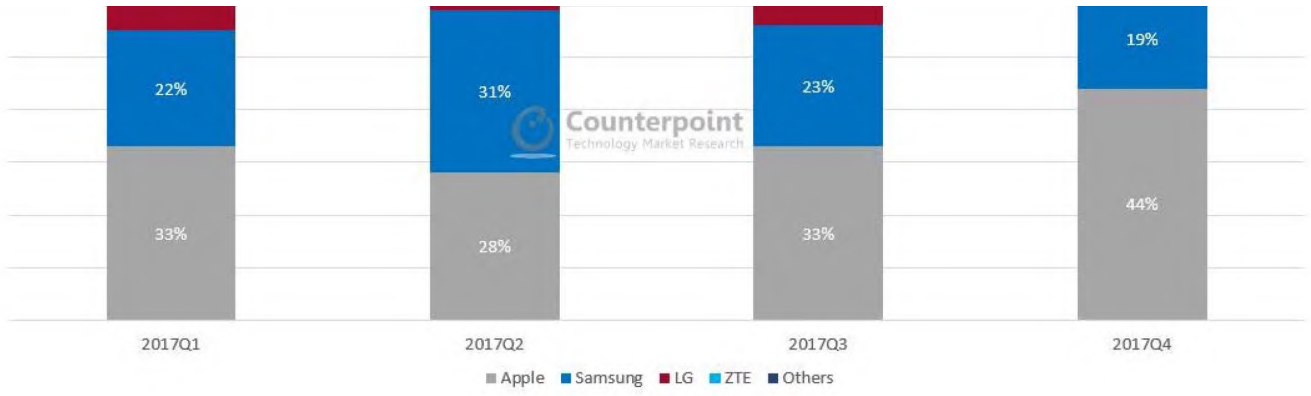
US Smartphone Shipments Market Share (%)	2017Q1	2017Q2	2017Q3	2017Q4	2018Q1
Apple	33%	28%	33%	44%	37%
Samsung	22%	31%	23%	19%	26%
LG	18%	15%	18%	14%	14%
ZTE	10%	11%	12%	11%	11%
Others	17%	15%	14%	12%	12%

Ranking is according to latest quarter.

Q4 2017 Highlights

- US smartphone market witnessed a record holiday quarter shipment, driven mainly by Apple.
- Apple posted a fourth quarter record as well in US, driven by the sales of its latest flagship offerings, iPhone X and iPhone 8 series smartphones.
- Samsung, LG, ZTE and Motorola followed Apple in the top 5 smartphone ranking respectively. Together the top 5 brands captured more than 90% of the total US smartphone market in Q4 2017.





US Smartphone Shipments Market Share (%)	2016 Q1	2016 Q2	2016 Q3	2016 Q4	2017 Q1	2017 Q2	2017 Q3	2017 Q4
Apple	33%	29%	33%	39%	33%	28%	33%	44%
Samsung	28%	30%	25%	19%	22%	31%	23%	19%
LG	14%	14%	13%	13%	18%	15%	18%	14%
ZTE	7%	10%	9%	11%	10%	11%	12%	11%
Others	18%	17%	20%	18%	17%	15%	14%	12%

MARKET SHARE | MARKET SHARE BY QUARTER | SMARTPHONE MARKET SHARE | SMARTPHONES | USA | US SMARTPHONE MARKET SHARE

Team Counterpoint

Counterpoint research is a young and fast growing research firm covering analysis of the tech industry. Coverage areas are connected devices, digital consumer goods, software & applications and other adjacent topics.

for high precision projects.

ALL AUTHOR POSTS

1 Comment counterpointresearch.com 1 Login

Recommend Tweet Share Sort by Best

Join the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Bowen Wang • 5 days ago

Where did you get the data

• Reply • Share ›

Subscribe Add Disqus to your siteAdd DisqusAdd Disqus' Privacy PolicyPrivacy PolicyPrivacy

Search...

Your Email

SUBSCRIBE

Exhibit 14-V

"DoD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices"

DOD Issues Cybersecurity Warning Against Lenovo Computers, Handheld Devices

Written by FEDmanager (/component/contact/contact/11?Itemid=101) on 25 October 2016.

The Department of Defense is concerned that computers and handheld devices produced by China-based company Lenovo could be used to spy on Pentagon networks, according to a recent internal study.

The report, produced last month by the J-2 intelligence directorate, also warned that Lenovo is looking to buy American IT firms that would give the company better access to the Pentagon's classified information and introduce compromised hardware into the Defense Department networks, posing cyber espionage risks.

"Although we are concerned any time another nation or individual attempts to initiate intelligence collection against the Department of Defense, we do not discuss internal assessments," said a **Joint Staff spokesman (http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/)**.

The J-2 report also contained a warning that Lenovo was seeking to purchase American information technology companies in a bid to gain access to classified Pentagon and military information networks.

In the past, Lenovo equipment was detected "beaconing," or secretly communicating with remote users during the course of cyber intelligence-gathering, according to one official who added that "There is no way that that company or any Chinese company should be doing business in the United States after all the recent hacking incidents."

According to the Washington Free Beacon, "about 27 percent of Lenovo Group Ltd. is owned by the Chinese Academy of Science, a government research institute. In April, a Chinese Academy of Sciences space imagery expert, Zhou Zhixin, **was named (http://news.ifeng.com/a/20160409/48403966_0.shtml)** to a senior post in the Chinese military's new Strategic Support Force, a unit in charge of space, cyber, and electronic warfare."

A spokesperson with the Pentagon said the Defense Department has not imposed a blanket ban on all Lenovo products, and does not blacklist suppliers or individual products.

The National Security Agency has previously linked China to cyber spying reports against the Pentagon, as well as U.S. and foreign defense contractors, the report stated.

News of the internal study comes days after House Judiciary Chairman Bob Goodlatte **questioned (https://www.politicopro.com/cybersecurity/whiteboard/2016/10/house-chair-questions-clinton-advisers-use-of-chinese-computer-078828)** the FBI for more details about a senior Clinton campaign adviser who used a Lenovo computer to sort her personal from her private emails.

Photo: "Lenovo Laboratory (https://www.flickr.com/photos/fotois/4759074222/in/photolist-8fubzr-8fxsBY-8fxsHu-8fub5D-8fubkp-8fxsnq-8fxsgy-8fubtk-8fxs8o-8fxuXQ-8fud7H-8fucZZ-8fubev-8fudWv-8fud4x-8fxv2U)" by 246-You (https://www.flickr.com/photos/fotois/) is licensed under CC By 2.0 (https://creativecommons.org/licenses/by/2.0/)/ Cropped from original

Posted in General News (/featured/9-general-news)

Tags: cybersecurity (/component/tags/tag/cybersecurity), Federal IT Strategy (/component/tags/tag/federal-it-strategy), DOD (/component/tags/tag/dod), Department of Defense (/component/tags/tag/department-of-defense), Federal IT (/component/tags/tag/federal-it), china (/component/tags/tag/china)

Print

Exhibit 14-W

Backgrounder, Alcatel-Lucent Enterprise

Backgrounder

Approved for internal and external communication

100 years of innovation, pioneering and setting the course of history

In 2019 ALE celebrates its centenary. For a hundred years ALE and its people have made communication a reality. We invite you to join us on a historical journey which makes ALE the great company it is today.

When we look at our heritage and the 100-year journey, it's easy to see why our people are such pioneers and innovators. It's in the company DNA. It all began in 1919 in the Alsace region when Aaron Weil created a little company called **Le Téléphone Privé** changing the history of telecommunications.

During the 1920s and 30s, the company grew and took the name of **Téléphonie Industrielle et Commerciale** (**Télic**). In 1947, a subsidiary of **Télic** called **Alsatel** (**Société Alsacienne et Lorraine de Télécommunication et d'Electronique**) was created to enable sales expansion. These two companies worked hand in hand. In 1954, **Télic** started to expand with the acquisition of **Cofratel** (**Compagnie Française du Téléphone**). In 1960, **Télic** led the world by delivering the complex Crossbar Telephony technology. Impressed, **CGE** decided to acquire **Télic** under its **Compagnie Industrielle de Téléphone** (**CIT**) division. **CGE** would go on to become a leader in digital communications and would also be known for producing cables, power plants and the TGV high-speed trains in France.

In 1970, a defining moment occurred with the creation of **Alcatel** by merging the **CIT** and **ENTE** (**Énergie Nucléaire Télécommunications et Electronique**), a division of the **Société Alsacienne de Constructions Mécaniques** (**SACM**). **Alcatel** stands for **Alsacienne de Constructions Atomiques, de Télécommunications et d'Electronique**.

In 1980 **Télic**, still a part of **CIT**, changed its name to **Télic-Alcatel**. In the same year **Télic-Alcatel** pioneered and introduced the Minitel, a Videotext online service accessible through telephone lines.

In 1987, a major merger took place between **CGE** and the **ITT** group bringing European centric regions and US and China centric regions together to develop worldwide reach. **Télic-Alcatel's** portfolio merged with the **ITT** group.

In 1991, at parent level, **CGE** became **Alcatel Alsthom**, and at Enterprise level, **Telic-Alcatel** and sister companies (**Bell** and **SEL**) became **Alcatel Business Systems**. The portfolio of voice solutions created at this time lives on in our portfolio of today. In 1991, we proudly launched the first ISDN Videophone with a proprietary VLSI (very large-scale integration) silicon chip, at a time when very few companies were able to design silicon chips.

In 1997, **Alcatel Business Systems** in partnership with **Sun Microsystems** launched the first internet screen phone in Java technology.

One year later, in 1998, the parent company **Alcatel Alsthom** abbreviated its name to **Alcatel** to focus on telecommunications as its core business. An acquisition opportunity arose in 1999 to acquire American companies **Xylan**, **Packet Engines, Assured Access and Internet Devices**, all companies specializing in enterprise network solutions. These companies were merged into the **Alcatel Business Systems** company which would become **Alcatel-Lucent Enterprise** in 2011.

100 Years Backgrounder

Backgrounder

Approved for internal and external communication

In 2006, the parent company **Alcatel** and **Lucent Technologies** merged to become the modern **Alcatel-Lucent**, a telecommunications giant, today part of **Nokia**. In 2014, via a carve out, **Alcatel-Lucent Enterprise** was acquired by **China Huaxin Post & Telecommunication Economy Development Center**. We have since introduced our Hybrid Cloud Communication solutions, persistent Team Messaging, and the first open CPaaS platform, as well as unified access for wired and wireless networks and intelligent fabric to automate network deployments.

In 2019 our centenary program takes us through this journey and beyond, looking into the future to explore new technologies born from a unique heritage and expertise. We look at what the next 100 years might bring as ALE continues to lead the world in B2B digital transformation, cloud, vertical solutions and the Internet of Things.

Additional information
Word count: 602

Exhibit 14-X

Alpha Networks, Inc.'s "Design Manufacturing, Service (DMS)" Webpage

About Alpha

Design , Manufacturing, Service (DMS)

Founded	September, 2003
Headquarter	Hsinchu Science Park, Taiwan
IPO	2004, Taiwan Stock Exchange
Paid-in-Capital	NT$ 5.44 bln (US$ 186 mln)
Number of Employees	More than 3,500
R&D Centers	Hsinchu, Taiwan; Taipei, Taiwan; Chengdu, China; Irvine, U.S.A.
Manufacturing Locations	Hsinchu, Taiwan; Dongguan, China; Changshu, China
Sales Locations	Taiwan, U.S.A., Japan, and China
Business Model	Design、Manufacturing、Service (DMS)

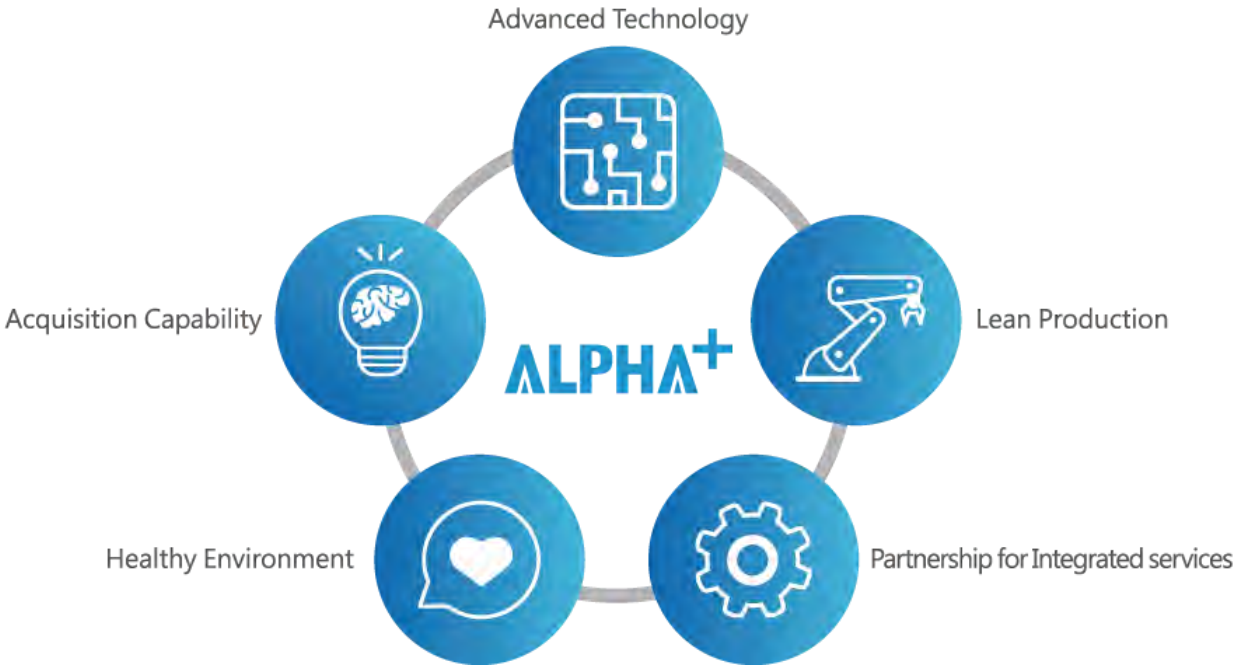
Vision

Forge the Internet to connect people and things.

Mission

Alpha Networks is a globally recognized, professional networking DMS supplier.
We use advanced technology to provide our customers with outstanding solutions at the best value.

Alpha+ Strategy



Alpha Values

Ethics

We value integrity and lead by example.We commit to strict confidentiality and avoid all conflicts of interest.

Customer Values

We put the values and needs of our customers first and commit to deliver.

Agility

We respond swiftly to customer needs and identify market trends to develop the best solutions.

Network Performance

We fully optimize the networking process to generate the optimal outcome.

+886-3-563-6666

No.8 Li-shing 7th Rd., Science-based Industrial Park, Hsinchu, Taiwan, R.O.C

Copyright ©Alpha Networks Inc. All rights reserved. Designed by Weya.

Exhibit 14-Y

Alpha Networks, Inc.'s "About Alpha" Webpage

ABOUT ALPHA

A Networking DMS Leader with Global Experience

Founded in September 2003, as a spin-off from the D-Link Corporation, Alpha Networks Inc. offers customers nearly 30 years of experience in the networking industry. Alpha possesses highly capable design, manufacturing, and service resources in networking products and offers a complete portfolio of off-the-shelf and custom solutions. Since its inception, Alpha Networks has enjoyed consistent, strong growth and successfully built its reputation by delivering comprehensive product portfolios that deploy a variety of mature and cutting edge technologies. Additionally, by leveraging market intelligence and global experience derived from solid partnerships with first-tier brand name companies, Alpha Networks has proved itself capable of developing design and manufacturing expertise that often push the boundaries of innovation and have helped to elevate Alpha Networks to a position of global leadership in the networking industry.

About Alpha

Our guidance is Integrity, Teamwork, Excellence, Innovation.

Milestones

Milestone timeline of Alpha Networks's success.

Global Presence

Macroscopic Overview with Local Support.

Contact Us

繁 简

+886-3-563-6666

No.8 Li-shing 7th Rd., Science-based Industrial Park, Hsinchu, Taiwan, R.O.C

Copyright ©Alpha Networks Inc. All rights reserved. Designed by Weya.

GPL Source Code Statement

Exhibit 14-Z

Excerpts from Arista Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

Or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission file number: 001-36468

ARISTA NETWORKS, INC.

(Exact name of registrant as specified in its charter)

Delaware	**20-1751121**
(State or other jurisdiction of incorporation or organization)	**(I.R.S. Employer Identification Number)**

5453 Great America Parkway
Santa Clara, California 95054
(Address of principal executive offices)

(408) 547-5500
(Registrant's telephone number, including area code)
Securities registered pursuant to Section 12(b) of the Act:

Title of each class	**Name of each exchange on which registered**
Common Stock, $0.0001 par value	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Exchange Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See definitions of "large accelerated filer," "accelerated filer," "smaller reporting company" and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☒	Accelerated filer ☐
Non-accelerated filer ☐	Smaller reporting company ☐
	Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of the registrant's common stock held by non-affiliates of the registrant was approximately $14,715,944,627 as of June 30, 2018 b ased on the closing sale price of the registrant's common stock on the New York Stock Exchange on such date. Shares held by persons who may be deemed affiliates have been excluded. This determination of affiliate status is not necessarily a conclusive determination for other purposes.

On February 8, 2019 , 75,730,873 shares of the registrant's common stock were outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive Proxy Statement relating to its 2019 Annual Stockholders' Meeting to be filed pursuant to Regulation 14A within 120 days after the registrant's fiscal year end of December 31, 2018 are incorporated by reference into Part III of this Annual Report on Form 10-K.

Our Market Opportunity

We compete primarily in the data center switching market for 10 Gigabit Ethernet and above, excluding blade switches. We also compete in the enterprise campus market for 1 Gigabit Ethernet switching and above and cloud-managed wireless networking.

We believe that cloud computing represents a fundamental shift from traditional legacy data centers and that cloud networking is the fastest growing segment within the data center switching market. As organizations of all sizes are adopting cloud architectures, spending on cloud and next-generation data centers has increased rapidly over the last several years, while traditional legacy IT spending has been growing more slowly. Our 7150, 7050, 7250, 7300 and 7500 Series platforms are now listed on the U. S. Department of Defense Approved Products Lists Integrated Tracking System by the Defense Information Systems Agency.

Our Customers

As of December 31, 2018 , we had delivered our cloud networking solutions to over 5,500 end customers worldwide in approximately 86 countries. Our end customers span a range of industries and include large internet companies, service providers, financial services organizations, government agencies, media and entertainment companies and others. For each of the years ended December 31, 2018 , 2017 , and 2016 , Microsoft purchases, through our channel partner World Wide Technology, Inc., accounted for more than 10% of our total revenue.

Our Competitive Strengths

We believe the following strengths will allow us to maintain and extend our technology leadership position in cloud networking and next-generation data center Ethernet products:

- ***Purpose-Built Cloud Networking Platform.*** We have developed a highly scalable cloud networking platform that uses software to address the needs of large-scale internet companies, cloud service providers, financial services organizations, government agencies and media and entertainment companies, including virtualization, big data and low-latency applications. As a result, our cloud networking platform does not have the inherent limitations of legacy network architectures.
- ***Broad and Differentiated Portfolio.*** Using multiple silicon architectures, we deliver switches and routers with industry-leading capacity, low latency, port density and power efficiency and have innovated in areas such as deep packet buffers, embedded optics and reversible cooling. Our broad portfolio has allowed us to offer customers products that best match their specific requirements.
- ***Single Binary Image Software.*** The single binary image of EOS software allows us to maintain feature consistency across our entire product portfolio and enables us to introduce new software innovations into the market that become available to our entire installed base without a “forklift upgrade” (i.e., a broad upgrade of the data center infrastructure).
- ***Rapid Development of New Features and Applications.*** Our highly modular EOS software has allowed us to rapidly deliver new features and applications while preserving the structural integrity and quality of our network operating system. We believe our ability to deliver new features and capabilities more quickly than legacy switch/router operators, provides us with a strategic advantage given that the requirements in cloud and next-generation data center networking continue to evolve rapidly.
- ***Deep Understanding of Customer Requirements.*** We have developed close working relationships with many of our largest customers that provide us with insights about their needs and future requirements. This has allowed us to develop and deliver products to market that meet customer demands and expectations as well as to rapidly grow sales to existing customers.
- ***Strong Management and Engineering Team with Significant Data Center Networking Expertise.*** Our management and engineering team consists of networking veterans with extensive data center networking expertise. Our President and Chief Executive Officer, Jayshree Ullal, with 30+ years of networking expertise from silicon to systems companies. Andy Bechtolsheim, our Founder and Chief Development Officer, was previously a Founder and chief system architect at Sun Microsystems. Kenneth Duda, our Founder and Chief Technology Officer, led the software development effort of EOS.

- ***Significant Technology Lead.*** We believe that our networking technology represents a fundamental advance in networking software. Our EOS software is state-driven and the result of more than 1,000 man-years of research and development investment over a ten-year period with 10+ million lines of code as a key cloud networking software stack.

Our Products and Technology

We offer one of the broadest product lines of data center 10/25/40/50/100 Gigabit Ethernet switches and routers in the industry, comprising our 7010/7020 Series, 7050X Series, 7060X Series, 7130 Series, 7160 Series, 7150 Series, 7170 Series, 7250X Series, 7260 Series, 7280R Series Universal Leaf products, 7300X Series Spline products, and our 7500R Series Universal Spine products.

We deliver routing and switching platforms with industry-leading capacity, low latency, port density and power efficiency. We have also innovated in areas such as deep packet buffers, embedded optics and reversible cooling. An overview of our switching/routing portfolio is shown in the figure below.

We use multiple silicon architectures across our products, which allows us to build a broader range of products optimized for different functions in the network than competitors that utilize fewer silicon architectures. While we use multiple silicon architectures, all of our platforms are powered with the same binary EOS image, which significantly simplifies deployment and ensures the same rich feature set and consistent operation across all our products.

Our Extensible Operating System

The core of our cloud networking platform is our Extensible Operating System, or EOS, which runs on top of standard Linux and offers programmability at all layers of the stack. All of our 10/25/40/50/100 Gigabit Ethernet platforms run our EOS software.

EOS is based on a new and innovative architecture that is highly modular and consists of more than 100 separate processes that we call agents, each one handling specific protocol processing, device driver or system management functions. Each agent runs in user space as a separate Linux process and is completely protected and isolated from all other agents.

We are constantly investing in our core infrastructure to provide the capabilities required for building modern cloud networks and enhancing scalability. New requirements for use in cloud and service provider networks and hybrid cloud deployments in enterprises require on-going upgrades and extensions to our state oriented architecture.

EOS Attributes

The modular and programmable architecture of EOS enables us to offer a set of attributes, capabilities and features that are essential for cloud networking and next-generation data centers.

- greater risk of unexpected changes in regulatory practices, tariffs and tax laws and treaties, including the Tax Act;
- greater risk of unexpected changes in tariffs imposed by the U.S. on goods from other countries and tariffs imposed by other countries on U.S. goods, including the tariffs recently implemented and additional tariffs that have been proposed by the U.S. government on various imports from China, Canada, Mexico and the EU, and by the governments of these jurisdictions on certain U.S. goods, and any other possible tariffs that may be imposed on services such as ours, the scope and duration of which, if implemented, remain uncertain;
- deterioration of political relations between the U.S. and Canada, the U.K., the EU and China, which could have a material adverse effect on our sales and operations in these countries;
- greater risk of changes in diplomatic and trade relationships, including new tariffs, trade protection measures, import or export licensing requirements, trade embargoes and other trade barriers;
- the uncertainty of protection for intellectual property rights in some countries;
- greater risk of a failure of foreign employees to comply with both U.S. and foreign laws, including antitrust regulations, the FCPA and any trade regulations ensuring fair trade practices; and
- heightened risk of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, or irregularities in, financial statements.

These and other factors could harm our ability to gain future international revenue and, consequently, materially affect our business, financial condition, results of operations and prospects. Expanding our existing international operations and entering into additional international markets will require significant management attention and financial commitments. Our failure to successfully manage our international operations and the associated risks effectively could limit our future growth or materially adversely affect our business, financial condition, results of operations and prospects.

Moreover, our business is also impacted by the negotiation and implementation of free trade agreements between the United States and other countries. Such agreements can reduce barriers to international trade and thus the cost of conducting business overseas. For instance, the United States recently reached a new trilateral trade agreement with the governments of Canada and Mexico to replace the North American Free Trade Agreement ("NAFTA"). If the United States withdraws from NAFTA and the three countries fail to approve the new agreements, known as the United States-Mexico-Canada Agreement, our cost of doing business within the three countries could increase.

The United Kingdom's vote to leave the European Union will have uncertain effects and could adversely affect us.

On June 23, 2016, the electorate in the United Kingdom, or UK, voted in favor of leaving the European Union, or EU, (commonly referred to as the "Brexit"). Thereafter, on March 29, 2017, the country formally notified the EU of its intention to withdraw pursuant to Article 50 of the Lisbon Treaty, triggering the two-year negotiation period for exiting the EU. The withdrawal of the UK from the EU is scheduled to take effect on March 29, 2019 either on the effective date of the withdrawal agreement or, in the absence of agreement, two years after the UK provides a notice of withdrawal pursuant to the EU Treaty and transitional provisions may or may not be put in place to ease the process.

The effects of Brexit will depend on agreements the UK makes to retain access to EU markets either during a transitional period or more permanently. Brexit creates an uncertain political and economic environment in the UK and potentially across other EU member states for the foreseeable future, including during any period while the terms of Brexit are being negotiated and such uncertainties could impair or limit our ability to transact business in the member EU states.

Further, Brexit could adversely affect European and worldwide economic or market conditions and could contribute to instability in global financial markets, and the value of the Pound Sterling currency or other currencies, including the Euro. We are exposed to the economic, market and fiscal conditions in the UK and the EU and to

changes in any of these conditions. Depending on the terms reached regarding Brexit, it is possible that there may be adverse practical and/or operational implications on our business.

A significant amount of the regulatory regime that applies to us in the UK is derived from EU directives and regulations. For so long as the UK remains a member of the EU, those sources of legislation will (unless otherwise repealed or amended) remain in effect. However, Brexit could change the legal and regulatory framework within the UK where we operate and is likely to lead to legal uncertainty and potentially divergent national laws and regulations as the UK determines which EU laws to replace or replicate. Consequently, no assurance can be given as to the impact of Brexit and, in particular, no assurance can be given that our operating results, financial condition and prospects would not be adversely impacted by the result.

Enhanced United States tax, tariff, import/export restrictions, Chinese regulations or other trade barriers may have a negative effect on global economic conditions, financial markets and our business.

There is currently significant uncertainty about the future relationship between the United States and various other countries, most significantly China, with respect trade policies, treaties, tariffs and taxes, including trade policies and tariffs regarding China. The current U.S. Administration has called for substantial changes to U.S. foreign trade policy with respect to China and other countries, including the possibility of imposing greater restrictions on international trade and significant increases in tariffs on goods imported into the United States. In 2018, the Office of the U.S. Trade Representative (the “USTR”) enacted tariffs on imports into the U.S. from China, including communications equipment products and components manufactured and imported from China. The tariff became effective on September 24, 2018, with an initial rate of 10% and was scheduled to increase from 10% to 25% on January 1, 2019; however, that increase has been delayed for 90 days pending trade negotiations between the U.S. and China. In addition, the tariffs may be increased in the future. It is expected that these tariffs will cause our costs to increase, which could narrow the profits we earn from sales of products requiring such materials. Furthermore, if tariffs, trade restrictions, or trade barriers are placed on products such as ours by foreign governments, especially China, the prices for our products may increase, which may result in the loss of customers and our business, financial condition and results of operations may be harmed. We believe we can adjust our supply chain and manufacturing practices to minimize the impact of the tariffs, but our efforts may not be successful, there can be no assurance that we will not experience a disruption in our business related to these or other changes in trade practices and the process of changing suppliers in order to mitigate any such tariff costs could be complicated, time-consuming, and costly.

Furthermore, the U.S. tariffs may cause customers to delay orders as they evaluate where to take delivery of our products in connection with their efforts to mitigate their own tariff exposure. Such delays create forecasting difficulties for us and increase the risk that orders might be canceled or might never be placed. Current or future tariffs imposed by the U.S. may also negatively impact our customers' sales, thereby causing an indirect negative impact on our own sales. Any reduction in our customers' sales, and/or any apprehension among distributors and customers of a possible reduction in such sales, would likely cause an indirect negative impact on our own sales. Even in the absence of further tariffs, the related uncertainty and the market's fear of an escalating trade war might cause our distributors and customers to place fewer orders for our products, which could have a material adverse effect on our business, liquidity, financial condition, and/or results of operations.

Additionally, the current U.S. Administration continues to signal that it may alter trade agreements and terms between China and the United States, including limiting trade with China, and may impose additional tariffs on imports from China. Therefore, it is possible further tariffs may be imposed that could cover imports of communications equipment products and components used in our products, or our business may be adversely impacted by retaliatory trade measures taken by China or other countries, including restricted access to suppliers, communications equipment products and components used in our products, causing us to raise prices or make changes to our products, which could materially harm our business, financial condition and results of operations. The current administration, along with Congress, has created significant uncertainty about the future relationship between the United States and other countries with respect to the trade policies, treaties, taxes, government regulations and tariffs that would be applicable. It is unclear what changes might be considered or implemented and what response to any such changes may be by the governments of other countries. These changes have created significant uncertainty about the future relationship between the United States and China, as well as other countries, including with respect to the trade policies, treaties, government regulations and tariffs that could apply to trade

- obsolescence charges;
- changes in shipment volume;
- the timing of revenue recognition and revenue deferrals;
- increased cost, loss of cost savings or dilution of savings due to changes in component pricing or charges incurred due to inventory holding periods if parts ordering does not correctly anticipate product demand or if the financial health of either contract manufacturers or suppliers deteriorates;
- increased costs arising from the tariffs imposed by the U.S. on goods from other countries and tariffs imposed by other countries on U.S. goods, including the tariffs recently implemented and additional tariffs that have been proposed by the U.S. government on various imports from China, Canada, Mexico and the E.U. and by the governments of these jurisdictions on certain U.S. goods;
- lower than expected benefits from value engineering;
- changes in distribution channels;
- increased warranty costs; and
- our ability to execute our strategy and operating plans.

We determine our operating expenses largely on the basis of anticipated revenues and a high percentage of our expenses are fixed in the short and medium term. As a result, a failure or delay in generating or recognizing revenue could cause significant variations in our operating results and operating margin from quarter to quarter. Failure to sustain or improve our gross margins reduces our profitability and may have a material adverse effect on our business and stock price.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, our sales and revenue are difficult to predict and may vary substantially from period to period, which may cause our results of operations to fluctuate significantly.

The timing of our sales and revenue recognition is difficult to predict because of the length and unpredictability of our products' sales cycles. A sales cycle is the period between initial contact with a prospective end customer and any sale of our products. End-customer orders often involve the purchase of multiple products. These orders are complex and difficult to complete because prospective end customers generally consider a number of factors over an extended period of time before committing to purchase the products and solutions we sell. End customers, especially in the case of our large end customers, often view the purchase of our products as a significant and strategic decision and require considerable time to evaluate, test and qualify our products prior to making a purchase decision and placing an order. The length of time that end customers devote to their evaluation, contract negotiation and budgeting processes varies significantly. Our products' sales cycles can be lengthy in certain cases, especially with respect to our prospective large end customers. During the sales cycle, we expend significant time and money on sales and marketing activities and make investments in evaluation equipment, all of which lower our operating margins, particularly if no sale occurs. Even if an end customer decides to purchase our products, there are many factors affecting the timing of our recognition of revenue, which makes our revenue difficult to forecast. For example, there may be unexpected delays in an end customer's internal procurement processes, particularly for some of our larger end customers for which our products represent a very small percentage of their total procurement activity. There are many other factors specific to end customers that contribute to the timing of their purchases and the variability of our revenue recognition, including the strategic importance of a particular project to an end customer, budgetary constraints and changes in their personnel.

Even after an end customer makes a purchase, there may be circumstances or terms relating to the purchase that delay our ability to recognize revenue from that purchase. In addition, the significance and timing of our product enhancements, and the introduction of new products by our competitors, may also affect end customers' purchases. For all of these reasons, it is difficult to predict whether a sale will be completed, the particular period in which a sale will be completed or the period in which revenue from a sale will be recognized. If our sales cycles lengthen, our revenue could be lower than expected, which would have an adverse effect on our business, financial condition, results of operations and prospects.

- a classified board of directors with three-year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our board of directors;
- the ability of our board of directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquirer;
- the exclusive right of our board of directors to elect a director to fill a vacancy created by the expansion of our board of directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our board of directors;
- a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders;
- the requirement that a special meeting of stockholders may be called only by the chairman of our board of directors, our president, our secretary or a majority vote of our board of directors, which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors;
- the requirement for the affirmative vote of holders of at least 66 2/3% of the voting power of all of the then outstanding shares of the voting stock, voting together as a single class, to amend the provisions of our amended and restated certificate of incorporation relating to the issuance of preferred stock and management of our business or our amended and restated bylaws, which may inhibit the ability of an acquirer to effect such amendments to facilitate an unsolicited takeover attempt;
- the ability of our board of directors, by majority vote, to amend the bylaws, which may allow our board of directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquirer to amend the bylaws to facilitate an unsolicited takeover attempt; and
- advance notice procedures with which stockholders must comply to nominate candidates to our board of directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer's own slate of directors or otherwise attempting to obtain control of us.

In addition, as a Delaware corporation, we are subject to Section 203 of the Delaware General Corporation Law. These provisions may prohibit large stockholders, in particular those owning 15% or more of our outstanding voting stock, from merging or combining with us for a certain period of time.

The issuance of additional stock in connection with financings, acquisitions, investments, our stock incentive plans or otherwise will dilute all other stockholders.

Our amended and restated certificate of incorporation authorizes us to issue up to 1,000,000,000 shares of common stock and up to 100,000,000 shares of preferred stock with such rights and preferences as may be determined by our board of directors. Subject to compliance with applicable rules and regulations, we may issue our shares of common stock or securities convertible into our common stock from time to time in connection with a financing, acquisition, investment, our stock incentive plans or otherwise. We may from time to time issue additional shares of common stock at a discount from the then market price of our common stock. Any issuance of stock could result in substantial dilution to our existing stockholders and cause the market price of our common stock to decline.

Item 1B. Unresolved Staff Comments

None.

Item 2. Properties

Our corporate headquarters is located in Santa Clara, California where we currently lease approximately 210,000 square feet of space under a lease agreement that expires in 2023. In addition, we lease office spaces for operations, sales personnel and research and development in locations throughout the U.S. and various international

locations, including Ireland, Canada, India, Australia, the United Kingdom, Korea, Singapore, Japan, Malaysia, China, Mexico, France, Taiwan, and United Arab Emirates. We also lease data centers in the U.S., Ireland and the United Kingdom.

We believe that our current facilities are adequate to meet our current needs. We intend to expand our facilities or add new facilities as we add employees and enter new geographic markets, and we believe that suitable additional or alternative space will be available as needed to accommodate ongoing operations and any such growth. We expect to incur additional expenses in connection with such new or expanded facilities.

Item 3. Legal Proceedings

The information set forth under the “Legal Proceedings” in Note 7. Commitments and Contingencies of the Notes to Consolidated Financial Statements included in Part II, Item 8, of this Annual Report on Form 10-K is incorporated herein by reference.

Item 4. Mine Safety Disclosures

Not applicable.

Exhibit 14-AA

Excerpts from Extreme Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended June 30, 2018

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

Form 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended June 30, 2018

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to .

Commission file number 000-25711

Extreme Networks, Inc.

(Exact name of Registrant as specified in its charter)

Delaware (State or other jurisdiction of incorporation or organization)	**77-0430270** (I.R.S. Employer Identification No.)
6480 Via del Oro **San Jose, California** (Address of principal executive offices)	**95119** (Zip Code)

Registrant's telephone number, including area code: (408) 579-2800

Securities registered pursuant to Section 12(b) of the Act: None
Securities registered pursuant to Section 12(g) of the Act:
Common stock, $0.001 par value

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☐ No ☒

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§229.405 of this chapter) is not contained herein, and will not be contained, to the best of registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant has submitted electronically and posted on its corporate Web site, if any, every Interactive Data File required to be submitted and posted pursuant to Rule 405 of Regulation S-T (§229.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit and post such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, smaller reporting company, or an emerging growth company. See the definitions of "large accelerated filer," "accelerated filer," "smaller reporting company," and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large Accelerated Filer	☒	Accelerated Filer	☐
Non-Accelerated Filer	☐	Smaller reporting company	☐
Emerging growth company	☐		

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of voting stock held by non-affiliates of the Registrant was approximately $1.2 billion as of December 31, 2017 the last business day of the Registrant's most recently completed second fiscal quarter, based upon the per share closing price of the Registrant's common stock as reported on The NASDAQ Global Market reported on such date. For purposes of this disclosure, shares of common stock held or controlled by executive officers and directors of the registrant and by persons who hold more than 5% of the outstanding shares of common stock have been treated as shares held by affiliates. This calculation does not reflect a determination that certain persons are affiliates of the Registrant for any other purpose.

118,320,200 shares of the Registrant's Common stock, $.001 par value, were outstanding as of August 24, 2018.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive proxy statement for the 2018 Annual Meeting of Stockholders to be filed with the Commission pursuant to Regulation 14A not later than 120 days after the end of the fiscal year covered by this Annual Report on Form 10-K are incorporated herein by reference in Part III of this Annual Report on Form 10-K.

- **The Internet of Things.** The Internet of Things is having dramatic effects on network infrastructure in healthcare, education, manufacturing, government and retail as more “smart” devices are entering the networks. These devices pose opportunities as well as threats to the network.
- **Growing usage of the cloud.** Enterprises have migrated increasing numbers of applications and services to either private clouds or public clouds offered by third parties. In either case, the network infrastructure must adapt to this new dynamic environment. Intelligence and automation are key if enterprises are to derive maximum benefit from their cloud deployments. Ethernet speeds, scaling from 10 Gigabits per second ("G") to 100G, provide the infrastructure for both private and public clouds. In addition, there is growing interest in SDN approaches that may include technologies such as OpenFlow, OpenStack, and CloudStack for increased network agility.
- **Vendor consolidation is expected to continue.** Consolidation of vendors within the enterprise network equipment market and between adjacent markets (storage, security, wireless & voice software and applications) continues to gain momentum. We identified this trend in 2013 with our acquisition of Enterasys. Further, we believe customers are demanding more end-to-end, integrated networking solutions. To address this demand, we acquired the WLAN Business of Zebra in October 2016, the Campus Fabric Business from Avaya in July 2017, and the Data Center Business from Brocade in October 2017.

Our strategy, product portfolio and research and development are closely aligned with what we have identified as the following trends in our industry:

- **The software segment of the worldwide enterprise network equipment market has continued to evolve and demands for improvements in Network Management will continue.**
  - *We announced our Extreme Management Console in Fiscal 2017. This innovative software helps IT network administrators to navigate the unprecedented demands caused by the surge of IoT devices and technology.*
- **Enterprise adoption of the cloud and open-source options are disrupting traditional license and maintenance business models.**
  - *We announced cloud offerings in April 2016 and enhanced those offerings in 2017. Extreme began participation in the OpenSwitch program in May 2016 and now participates in the StackStorm community with the acquisition from Brocade in November 2017.*
- **Enterprise adoption of new financing solutions allows for increased flexibility, Limited investment and zero long-term commitments. These offerings are changing the traditional CAPEX model to (OPEX) models using financing purchases over time are disrupting traditional sell-in business models.**
  - *We announced Extreme Capital Solutions in April 2018. The offering includes subscription, capital leasing and usage business models that provide flexibility for partners and customers.*
- **Growth of wireless devices continues to outpace hardwire switch growth.**
  - *We announced our 802.11ac Wave 2 wireless offering in late 2015 and plans to continue to advance our wireless portfolio of indoor and outdoor access points.*

The Extreme Strategy

We are focused on delivering end-to-end IP networking solutions for today’s enterprise environments. From wireless and wired access technologies, through the campus, core and into the datacenter, Extreme is developing solutions to deliver outstanding business outcomes for our customers. Leveraging a unified management approach, both on premise and in the cloud, we continue to accelerate adoption and delivery of new technologies in support of emerging trends in enterprise networking. We continue to execute on our growth objectives by maximizing customer, partner, and shareholder value.

In fiscal 2014, we completed the acquisition of Enterasys Networks. In fiscal 2017, we completed the acquisition of the WLAN Business from Zebra. In fiscal 2018, we completed the acquisitions of the Campus Fabric Business from Avaya and the Data Center Business from Brocade. These acquisitions support our growth strategy to lead the enterprise network equipment market with end-to-end software-driven solutions for enterprise customers from the data center to the wireless edge. After the closing of the acquisitions of the Campus Fabric Business and Data Center Business, Extreme immediately became a networking industry leader with more than 30,000 customers. As a network switching leader in enterprise, datacenter and cloud, after closing of the Campus Fabric Business, we combine and extend our world-class products and technologies to provide customers with some of the most advanced, high performance and open solutions in the market as well as a superb overall customer experience. The combination of Extreme, the Campus Fabric Business and the Data Center Business is significant in that it brings together distinct strengths addressing the key areas of the network, from unified wired and wireless edge, to the enterprise core, to the data center and cloud to offer a complete, unified portfolio of software-driven network access solutions.

Provider of high quality, software-driven, secure networking solutions and the industry's #1 customer support organization

- Only multi-vendor network management with "single pane of glass".
- Delivering new releases of next generation portfolio organically and through acquisition.

Key elements of our strategy include:

- **Focus on being nimble and responsive to customers and partners, we call this "Customer-Driven Networking™."** We work with our customers to deliver software-driven solutions from the enterprise edge to the cloud that are agile, adaptive, and secure to enable digital transformation for our customers. We help our customers move beyond just "keeping the lights on", so they can think strategically and innovate. By allowing customers to access critical decision-making intelligence, we are able reduce their daily tactical work so they can spend their time on learning and understanding how to innovate their business with IT.
- **Enable a common fabric to simplify and automate the network.** With the acquisition of the Campus Fabric Business, Extreme now has access to field driven Campus and Data Center Fabric technologies. Fabric technologies virtualize the network infrastructure (decoupling network services from physical connectivity) which enables network services to be turned up faster, with lower likelihood of error. They make the underlying network much easier to design, implement, manage and troubleshoot.
- **Software-driven networking services-led solutions.** Our software-driven solutions provide visibility, control and strategic intelligence from the Edge to the Data Center, across networks and applications. Our solutions include wired switching, wireless switching, wireless access points and controllers. We offer a suite of products that are tightly integrated with access control, network and application analytics as well as network management. All can be managed, assessed and controlled from one single pane of glass.
- **Offer customers choice – cloud or on premise.** We leverage cloud where it makes sense for our customers and provide on premise solutions where customers need it. Our hybrid approach gives our customers options to adapt the technology to their business. At the same time, all of our solutions have visibility, control and strategic information built in, all tightly integrated with one single pane of glass. Our customers can understand what's going on across the network and applications in real time – who, when, and what is connected to the network, which is critical for BYOD and IoT.
- **Enable IoT without additional IT resources.** In a recent IoT IT infrastructure survey conducted in December 2016, enterprise IT decision makers across industry verticals indicated their preference to opt for their existing wireless connectivity infrastructure to support IoT devices. These preferences will place unprecedented demand on network administrators to enhance management capabilities, scalability and programmability of the enterprise networks they manage without additional IT resources.
- **Provide a strong value proposition for our customers.** Our cloud-managed wired and wireless networking solutions that provide additional choice and flexibility with on or off premise network, device and application management coupled with our award-winning services and support provide a strong value proposition to the following customers and applications:
  - Enterprises and private cloud data centers use our products to deploy automated next-generation virtualized and high-density infrastructure solutions.
  - Enterprises and organizations in education, healthcare, manufacturing, hospitality, transportation and logistics and government agencies use our solutions for their mobile campus and backbone networks.
  - Enterprises, universities, healthcare and hospitality organizations use our solutions to enable better visibility and control of their data processing and analytics requirements.
- **Provide high-quality customer service and support.** We seek to enhance customer satisfaction and build customer loyalty through high-quality service and support. This includes a wide range of standard support programs that provide the level of service our customers require, from standard business hours to global 24-hour-a-day, 365-days-a-year real-time response support.

- **Extend switching and routing technology leadership.** Our technological leadership is based on innovative switching, routing and wireless products, the depth and focus of our market experience and our operating systems - the software that runs on all of our Ethernet Switches. Our products reduce operating expenses for our customers and enable a more flexible and dynamic network environment that will help them meet the upcoming demands of IoT, mobile, and cloud, etc. Furthermore, our network operating systems, our primary merchant silicon vendor, and select manufacturing partners permit us to leverage our engineering investment. We have invested in engineering resources to create leading-edge technologies to increase the performance and functionality of our products, and as a direct result, the value of our solution to our current and future customers. We look for maximum synergies from our engineering investment in our targeted verticals.
- **Expand Wi-Fi technology leadership.** Wireless is today's network access method of choice and every business must deal with scale, density and BYOD challenges. The increase in demand being seen today, fueled by more users with multiple devices, increases the expectation that everything will just work. The network edge landscape is changing as the explosion of mobile devices increases the demand for mobile, transparent and always-on wired to wireless edge services. This new "unified access layer" requires distributed intelligent components to ensure that access control and resiliency of business services are available across the entire infrastructure and manageable from a single console. Our unified access layer portfolio provides intelligence for the wired/wireless edge
- **Continue to deliver unified management and a common fabric across the wired/wireless environment from the Data Center to the mobile Edge.** Our rich set of integrated management capabilities provides centralized visibility and highly efficient anytime, anywhere control of enterprise wired and wireless network resources.
- **Offer a superior quality of experience.** Our network-powered application analytics provide actionable business insight by capturing and analyzing context-based data about the network and applications to deliver meaningful intelligence about applications, users, locations and devices. With an easy to comprehend dashboard, our applications help businesses to turn their network into a strategic business asset that helps executives make faster and more effective decisions.

  Data can be mined to show how applications are being used enabling a better understanding of user behavior on the network, identifying the level of user engagement and assuring business application delivery to optimize the user experience. Application adoption can be tracked to determine the return on investment associated with new application deployment.

  Visibility into network and application performance enables our customers to pinpoint and resolve performance bottlenecks in the infrastructure whether they are caused by the network, application or server. This saves both time and money for the business and ensures critical applications are running at the best possible performance.
- **Software-driven networking solutions for the enterprise.** We are a software-driven networking solution company focused on the enterprise. We focus our R&D team and our sales teams to execute against a refined set of requirements for optimized return on investment, faster innovation, and clearer focus on mega trends and changes in the industry. As a software-driven networking company, we offer solutions for the entire enterprise network, the data center, the campus, the core and the WLAN.
- **Expand market penetration by targeting high-growth market segments.** Within the Campus, we focus on the mobile user, leveraging our automation capabilities and tracking WLAN growth. Our Data Center approach leverages our product portfolio to address the needs of public and private Cloud Data Center providers. Within the Campus we also target the high-growth physical security market, converging technologies such as Internet Protocol ("IP") video across a common Ethernet infrastructure in conjunction with technology partners.
- **Leverage and expand multiple distribution channels.** We distribute our products through select distributors, a large number of resellers and system-integrators worldwide, and several large strategic partners. We maintain a field sales force to support our channel partners and to sell directly to certain strategic accounts. As an independent Ethernet switch vendor, we seek to provide products that, when combined with the offerings of our channel partners, create compelling solutions for end-user customers.
- **Maintain and extend our strategic relationships.** We have established strategic relationships with a number of industry-leading vendors to both provide increased and enhanced routes to market, but also to collaboratively develop unique solutions.

We seek to differentiate ourselves in the market by delivering a value proposition based on a software-driven approach to network management, control and analytics.

Competition

The market for network switches, routers and software (including analytics) which is part of the broader market for networking equipment is extremely competitive and characterized by rapid technological progress, frequent new product introductions, changes in customer requirements and evolving industry standards. We believe the principal competitive factors in this market are:

- expertise and familiarity with network protocols, network switching/routing/wireless and network management;
- expertise and familiarity with application analytics software;
- expertise with network operations and management software;
- expertise in machine learning and artificial intelligence;
- product performance, features, functionality and reliability;
- price/performance characteristics;
- timeliness of new product introductions;
- adoption of emerging industry standards;
- customer service and support;
- size and scope of distribution network;
- brand name;
- breadth of product offering;
- access to customers; and
- size of installed customer base.

We believe we compete with our competitors with respect to many of the foregoing factors. However, the market for network switching solutions is dominated by a few large companies, particularly Cisco Systems, Inc., Dell, Hewlett-Packard Enterprise Co., Huawei Technologies Co. Ltd., Arista Networks Inc., Arris Corporation, and Juniper Networks Inc. Most of these competitors have longer operating histories, greater name recognition, larger customer bases, broader product lines and substantially greater financial, technical, sales, marketing and other resources.

We expect to face increased competition from both traditional networking solutions companies and Cloud platform companies offering Infrastructure-as-a-Service ("IaaS") and Platform-as-a-Service ("PaaS") products to enterprise customers. In that regard, we expect to face increased competition from certain Cloud Computing companies such as Amazon Web Services ("AWS"), Microsoft ("Microsoft Azure"), and Google Inc. ("Google Cloud Platform") providing a cloud-based platform of data center compute and networking services for enterprise customers.

With the acquisitions of assets from Zebra, Avaya and Brocade, we believe Extreme is uniquely positioned to address the most pressing market needs from the campus to the data center. Although we believe that our solutions and strategy will improve our ability to meeting the needs of our current and potential customers we cannot guarantee future success.

Restructuring

Fiscal year 2016

During fiscal 2016, we continued to realign our operations by abandoning excess facilities, primarily in San Jose, California; Salem, New Hampshire and Morrisville, North Carolina in addition to other smaller leased locations. These excess facilities represented approximately 32% of the floor space in the aggregate at these locations and included general office and warehouse space.

Fiscal year 2017

During fiscal 2017, we continued to realign our operations by continuing to review our excess facilities, expected sublease income, and implemented a reduction-in-force. We subleased our previous headquarters location at Rio Robles Drive in San Jose, California ("Rio Robles") and moved into a larger location at 6480 Via del Oro in San Jose, California ("Via del Oro") acquired as part of the WLAN Business acquisition. Additionally, due to the acquisitions of the Campus Fabric Business and the Data Center Business, there was a need to accommodate the increase in headcount. To address this need, the Company reoccupied a majority of the previously exited space in its Salem, New Hampshire location. In addition, we announced a reduction-in-force during the fiscal year affecting 90 employees.

Cost of Revenues and Gross Profit

The following table presents the gross profit on product and service revenue and the gross profit percentage of net revenues for the fiscal years 2018, 2017 and 2016 (dollars in thousands):

	Year Ended				Year Ended			
	June 30, 2018	June 30, 2017 (As adjusted)	$ Change	% Change	June 30, 2017 (As adjusted)	June 30, 2016 (As adjusted)	$ Change	% Change
Gross profit:								
Product	$ 407,393	$ 240,204	$167,189	69.6%	$ 240,204	$ 181,340	$ 58,864	32.5%
Percentage of product revenue	53.3%	52.2%			52.2%	46.9%		
Service	127,124	90,753	36,371	40.1%	90,753	84,063	6,690	8.0%
Percentage of service revenue	58.1%	61.9%			61.9%	63.2%		
Total gross profit	$ 534,517	$ 330,957	$203,560	61.5%	$ 330,957	$ 265,403	$ 65,554	24.7%
Percentage of net revenue	54.4%	54.5%			54.5%	51.1%		

Cost of product revenues includes costs of materials, amounts paid to third-party contract manufacturers, costs related to warranty obligations, charges for excess and obsolete inventory, scrap, distribution, product certification, amortization of developed technology intangibles, royalties under technology license agreements, and internal costs associated with manufacturing overhead, including management, manufacturing engineering, quality assurance, development of test plans, and document control. We outsource substantially all of our manufacturing. We conduct supply chain management, quality assurance, manufacturing engineering and document control at our facilities in San Jose, California, Salem, New Hampshire, China, and Taiwan.

Product gross profit increased to $407.4 million for the year ended June 30, 2018, from $240.2 million in the corresponding period of fiscal 2017, primarily due to higher revenues attributed to the acquisitions of the WLAN, the Campus Fabric and the Data Center Businesses and lower production costs due to cost reduction efforts. The increases in product gross profit were partially offset by increases in amortization of developed technology intangibles of $9.9 million, warranty charges of $7.2 million, royalty charges of $2.2 million and acquisition and integration related costs of $7.7 million including excess inventory charges related to the discontinuance of certain product lines due to the acquisitions of the Campus Fabric and the Data Center Businesses in excess of the same charges incurred related to the acquisition of the WLAN Business in the corresponding period in fiscal 2017.

Product gross profit increased to $240.2 million for the year ended June 30, 2017, from $181.3 million in the corresponding period of fiscal 2016. Product gross profit for the year ended June 30, 2017, was favorably impacted by an increase in product revenue of $73.5 million due primarily to the acquisition of the WLAN Business, lower amortization of developed technology intangibles of $8.3 million and more favorable manufacturing costs due to cost reduction efforts and lower warranty charges of $2.2 million. The increases in product gross profit were partially offset by integration costs of $5.0 million primarily related to excess inventory charges related to the discontinuance of certain product lines due to the WLAN Business acquisition and increased royalty charges of $2.6 million.

Our cost of service revenue consists primarily of labor, overhead, repair and freight costs and the cost of service parts used in providing support under customer maintenance contracts.

Service gross profit increased to $127.1 million for the year-ended June 30, 2018, from $90.8 million in the corresponding period of fiscal 2017, primarily due to the acquisitions of the WLAN, Campus Fabric and Data Center Businesses as a result of a higher number of maintenance contracts.

Service gross profit increased to $90.8 million for the year ended June 30, 2017, from $84.1 million in the corresponding period of fiscal 2016, primarily due to an increase in service revenue of $6.7 million related to the acquisition of the WLAN Business and the increased number of service contracts acquired.

Exhibit 14-BB

Excerpts from Juniper Networks, Inc.'s Form 10-K Annual Report for the Fiscal Year Ended Dec. 31, 2018

UNITED STATES SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended December 31, 2018

or

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from_____ to_____

Commission file number 001-34501

JUNIPER NETWORKS, INC.

(Exact name of registrant as specified in its charter)

Delaware	**77-0422528**
(State or other jurisdiction of incorporation or organization)	*(I.R.S. Employer Identification No.)*

1133 Innovation Way

Sunnyvale, California	**94089**
(Address of principal executive offices)	*(Zip code)*

(408) 745-2000

(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Name of each exchange on which registered
Common Stock, par value $0.00001 per share	New York Stock Exchange

Securities registered pursuant to Section 12(g) of the Act: None

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports), and (2) has been subject to such filings requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§ 232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark if disclosure of delinquent filers pursuant to Item 405 of Regulation S-K (§ 229.405 of this chapter) is not contained herein, and will not be contained, to the best of the registrant's knowledge, in definitive proxy or information statements incorporated by reference in Part III of this Form 10-K or any amendment to this Form 10-K. ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” “smaller reporting company”, and "emerging growth company" in Rule 12b-2 of the Exchange Act.

Large accelerated filer ☒	Accelerated filer ☐	Non-accelerated filer ☐	Smaller reporting company ☐	Emerging growth company ☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Act). Yes ☐ No ☒

The aggregate market value of voting common stock held by non-affiliates of the registrant was approximately $9,483,000,000 as of June 29, 2018, the last business day of the registrant’s most recently completed second fiscal quarter (based on the closing sales price for the common stock on the New York Stock Exchange on such date).

As of February 15, 2019, there were 347,922,460 shares of the registrant's common stock outstanding.

DOCUMENTS INCORPORATED BY REFERENCE

As noted herein, the information called for by Part III is incorporated by reference to specified portions of the registrant's definitive proxy statement to be filed in conjunction with the registrant's 2019 Annual Meeting of Stockholders, which is expected to be filed not later than 120 days after the registrant's fiscal year ended December 31, 2018.

Channel Sales Structure

A critical part of our sales and marketing efforts are our channel partners through which we conduct the majority of our sales. We utilize various channel partners, including, but not limited to the following:

- A global network of strategic distributor relationships, as well as region-specific or country-specific distributors who in turn sell to local VARs who sell to end-user customers. Our distribution channel partners resell routing, switching, and security products and services, which are purchased by all of our key customer verticals. These distributors tend to focus on particular regions or countries within regions. For example, we have substantial distribution relationships with Ingram Micro in the Americas and Hitachi in Japan. Our agreements with these distributors are generally non-exclusive, limited by region, and provide product and service discounts and other ordinary terms of sale. These agreements do not require our distributors to purchase specified quantities of our products or services. Further, most of our distributors sell our competitors' products and services, and some sell their own competing products and services.

- VARs and Direct value-added resellers, including our strategic worldwide alliance partners referenced below, resell our products to end-users around the world. These channel partners either buy our products and services through distributors, or directly from us, and have expertise in designing, selling, implementing, and supporting complex networking solutions in their respective markets. Our agreements with these channel partners are generally non-exclusive, limited by region, and provide product and service discounts and other ordinary terms of sale. These agreements do not require these channel partners to purchase specified quantities of our products or services. Increasingly, our Cloud and Service Provider customers also resell our products or services to their customers or purchase our products or services for the purpose of providing managed or cloud-based services to their customers.

- Strategic worldwide reseller relationships with established Juniper alliances, comprised of Dimension Data Holdings, or Dimension Data; Ericsson Telecom A.B., or Ericsson; International Business Machines, or IBM; and NEC Corporation. These companies each offer services and products that complement our own product and service offerings and act as a reseller, and in some instances as an integration partner for our products. Our arrangements with these partners allow them to resell our products and services on a non-exclusive and generally global basis, provide for product and service discounts, and specify other general terms of sale. These agreements do not require these partners to purchase specified quantities of our products or services.

Manufacturing and Operations

As of December 31, 2018, we employed 340 people in worldwide manufacturing and operations who manage our supply chain including relationships with our contract manufacturers, original design manufacturers, component suppliers, warehousing and logistics service providers.

Our manufacturing is primarily conducted through contract manufacturers and original design manufacturers in the United States, or U.S., China, Malaysia, Mexico, and Taiwan. As of December 31, 2018, we utilized Celestica Incorporated, Flextronics International Ltd., Accton Technology Corporation, and Alpha Networks Inc. for the majority of our manufacturing activity. Our contract manufacturers and original design manufacturers are responsible for all phases of manufacturing from prototypes to full production including activities such as material procurement, surface mount assembly, final assembly, test, control, shipment to our customers, and repairs. Together with our contract manufacturers and original design manufacturers, we design, specify, and monitor the tests that are required to ensure that our products meet internal and external quality standards. We believe that these arrangements provide us with the following benefits:

- We can quickly ramp up and deliver products to customers with turnkey manufacturing;

- We gain economies of scale by leveraging our buying power with our contract manufacturers and original design manufacturers when we manufacture large quantities of products;

- We operate with a minimum amount of dedicated space and employees for manufacturing operations; and

- We can reduce our costs by reducing what would normally be fixed overhead expenses.

Our contract manufacturers and original design manufacturers build our products based on our rolling product demand forecasts. Each contract manufacturer procures components necessary to assemble the products in our forecast and tests the products according to agreed-upon specifications. Products are then shipped to our distributors, VARs, or end-users. Generally, we do not own the components. Title to the finished goods is generally transferred from the contract manufacturers to us when the products leave the

We are dependent on contract manufacturers with whom we do not have long-term supply contracts, and changes to or disruptions in those relationships or manufacturing processes, expected or unexpected, may result in delays that could cause us to lose revenues and damage our customer relationships.

We depend on independent contract manufacturers (each of which is a third-party manufacturer for numerous companies) to manufacture our products. Although we have contracts with our contract manufacturers, these contracts do not require them to manufacture our products on a long-term basis in any specific quantity or at any specific price. In addition, it is time-consuming and costly to qualify and implement additional contract manufacturer relationships. Therefore, if we fail to effectively manage our contract manufacturer relationships, which could include failing to provide accurate forecasts of our requirements, or if one or more of them experiences delays, disruptions, or quality control problems in their manufacturing operations, or if we had to change or add additional contract manufacturers or contract manufacturing sites, our ability to ship products to our customers could be delayed. We have experienced in the past and may experience in the future an increase in the expected time required to manufacture our products or ship products. Such delays could result in supply shortfalls that damage our ability to meet customer demand for those products and could cause our customers to purchase alternative products from our competitors. Also, the addition of manufacturing locations or contract manufacturers or the introduction of new products by us would increase the complexity of our supply chain management. Moreover, a significant portion of our manufacturing is performed in China and other foreign countries and is therefore subject to risks associated with doing business outside of the United States, including import tariffs or regional conflicts. For example, the United States recently imposed a tariff on networking products imported from China; this includes certain products that we import into and sell within the United States. If we cannot mitigate the impact of the tariffs, the increased cost could translate into higher prices for our customers, reduced customer demand or increased cost of goods sold. In addition, increased costs of production or delays in production caused by any relocation of contract manufacturing facilities could impact the global competitiveness of our products. Each of these factors could adversely affect our business, financial condition and results of operations.

We are dependent on sole source and limited source suppliers, including for key components, which makes us susceptible to shortages, quality issues or price fluctuations in our supply chain, and we may face increased challenges in supply chain management in the future.

We rely on single or limited sources for many of our components. During periods of high demand for electronic products, component shortages are possible, and the predictability of the availability of such components may be limited. For example, we have recently experienced industry-wide supply constraints related to power management components. In addition, some components used in our networking solutions have in the past and may in the future experience extended lead times and higher pricing, given the demand in the market. Any future spike in growth in our business, the use of certain components we share in common with other companies, in IT spending or the economy in general, is likely to create greater short-term pressures on us and our suppliers to accurately forecast overall component demand and to establish optimal component inventories. If shortages or delays persist, we may not be able to secure enough components at reasonable prices or of acceptable quality to build and deliver products in a timely manner, and our revenues, gross margins and customer relationships could suffer. Additionally, if certain components that we receive from our suppliers have defects or other quality issues, we may have to replace or repair such components, and we could be subject to claims based on warranty, product liability, epidemic or delivery failures that could lead to significant expenses. We maintain product liability insurance, but there is no guarantee that such insurance will be available or adequate to protect against all such claims. We have experienced, and from time-to-time may experience, component shortages or quality issues that resulted, or could result, in delays of product shipments, revenue charges that impact our gross margins, and/or warranty or other claims or costs. We also currently purchase numerous key components, including ASICs and other semiconductor chips, from single or limited sources and many of our component suppliers are concentrated in China and Korea. In addition, there has been consolidation among certain suppliers of our components. For example, GLOBALFOUNDRIES acquired IBM's semiconductor manufacturing business, Avago Technologies Limited acquired Broadcom Corporation and Intel Corporation acquired Altera Corporation. Consolidation among suppliers can result in the reduction of the number of independent suppliers of components available to us, which could negatively impact our ability to access certain component parts or the prices we have to pay for such parts. In addition, our suppliers may determine not to continue a business relationship with us for other reasons that may be beyond our control. Any disruptions to our supply chain could decrease our sales, earnings and liquidity or otherwise adversely affect our business and result in increased costs. Such a disruption could occur as a result of any number of events, including, but not limited to, increases in wages that drive up prices, the imposition of regulations, quotas or embargoes on components, labor stoppages, transportation failures affecting the supply chain and shipment of materials and finished goods, third-party interference in the integrity of the products sourced through the supply chain, the unavailability of raw materials, severe weather conditions, natural disasters, civil unrest, military conflicts, geopolitical developments, war or terrorism and disruptions in utility and other services.

The development of alternate sources for components is time-consuming, difficult, and costly. In addition, the lead times associated with certain components are lengthy and preclude rapid changes in quantities and delivery schedules. Also, long-term supply and maintenance obligations to customers increase the duration for which specific components are required, which may further increase

Exhibit 14-CC

"OnePlus Breaks Into Top 5 Premium Phone Makers in US Market"

OnePlus Breaks Into Top 5 Premium Phone Makers in US Market

By Ryan Whitwam (https://www.extremetech.com/author/rwhitwam) on February 12, 2019 at 1:02 pm

21 Comments (https://www.extremetech.com/mobile/285635-oneplus-breaks-into-top-5-premium-phone-makers-in-us-market#disqus_thread)

27 SHARES

This site may earn affiliate commissions from the links on this page. **Terms of use (https://www.ziffdavis.com/terms-of-use#endorsement)**.

OnePlus popped up about five years ago, talking a big game about shaking up the phone industry. Those early attempts to get attention were pretty cringeworthy, but the company has matured over the years and started producing extremely competitive phones. The prices are higher than they once were, but OnePlus is still clocking in less expensive than the phones from Samsung, LG, and Google. This approach is working, too. OnePlus (https://www.extremetech.com/tag/oneplus) points to new numbers from IDC that show it among the top five premium smartphone makers in the US (https://www.digitaltrends.com/mobile/oneplus-top-five-us/).

According to the Q4 2018 numbers, OnePlus is now the fifth largest smartphone maker in the US market for phones costing more than $500. That puts it up there with Samsung and Apple. However, OP's overall ranking is lower when you factor in cheap phones, which still sell in large numbers as flagship phones get ever more costly.

OnePlus' journey to this point has been meteoric, but it hasn't been free of drama. OnePlus started with the OnePlus One, a phone that offered nearly flagship-level specs for just $299. In those early days, OnePlus used an invite system to limit costs. That made the phones harder to buy, but it *tried* to get people excited by running contests that encouraged people to break their old phones and women to post selfies. Yeah, those were bad ideas.

Not all the bumps in the road were OP's doing, though. It launched with the Cyanogen OS build of Android, but Cyanogen canceled that partnership just months later. That sent OnePlus scrambling to develop its own version of Android. It came up with Oxygen OS. The first few builds were a bit rough, but it's evolved into one of the best OEM Android skins on the market. Today, all of OnePlus' phones are powered by Oxygen OS.

~~(https://www.extremetech.com/wp-content/uploads/2018/08/587182-oneplus-6.jpg)~~

All OnePlus phones from OnePlus 3 onward were available without invites, but still only unlocked. The price also started to creep upward. The company still claimed strong sales, particularly in India.

The OnePlus 6T ~~launched late last year (https://www.extremetech.com/mobile/279976-the-oneplus-6t-launches-today-on-t-mobile-or-unlocked)~~, and this is what catapulted the company into the upper echelons of premium smartphone makers. At $550, the 6T is still several hundred dollars less

expensive than other high-end smartphones, and the compromises to reach that price are relatively minor. It's also available on T-Mobile, OP's first US carrier partnership. The unlocked version works on Verizon as well.

In the coming months, OnePlus is expected to release the OnePlus 7 with a notchless slider design. A separate 5G smartphone for select US carriers may also be in the cards.

Now read:

- ~~OnePlus 5 and 5T Will Get Faster Android Updates With Project Treble Support (https://www.extremetech.com/mobile/272885-oneplus-5-and-5t-will-get-faster-android-updates-with-project-treble-support)~~
- ~~OnePlus Will Be Among the First to Launch a 5G Phone (https://www.extremetech.com/mobile/279422-oneplus-will-be-among-the-first-to-launch-a-5g-phone)~~
- ~~Android or iOS: Who's Winning the Mobile Speed Race? (https://www.extremetech.com/mobile/263966-android-ios-whos-winning-global-speed-race)~~

1 Cool Thing: OnePlus 6

You Might Also Like

Powered By ZergNet

Exhibit 14-DD

"Who is BBK, The World's Third Largest Phone Manufacturer?"

Start typing...

Huawei ban OnePlus 7 Pro Google Pixel 3a Android Q Galaxy Fold
Galaxy S10

FEATURES NEWS October 20, 2017

Who is BBK, the world’s third largest phone manufacturer?

1.4K Shares

Robert Triggs

The smartphone market seems to be a perpetual fight for third place behind Samsung and Apple. Huawei has been trying to set itself up as the third largest brand, with successful pushes into the Asian, European, and now even U.S. markets. But they've got some relatively lesser-known competition to confront before they can claim the title of third— BBK Electronics.

BBK is a Chinese multinational corporation that owns a number of popular brands across various consumer electronics markets, including headphones, Blu-ray players, and smartphones. It owns two major smartphone brands and one fan favourite— Oppo, Vivo, and OnePlus.

Who is BBK?

BBK Electronics has been operating in various sections of China's electronics industry since around the 1990's. The company is spearheaded by reclusive billionaire Duan Yongping. After successfully generating more than 1 billion Yuan from the "Subor" gaming console, a competitor to the Nintendo Entertainment System, Duan left his position running a Chinese factory in 1995. He then started the company Bubugao, which would eventually become BBK. The company now owns factories spread over 10 hectares of land and more than 17,000 employees.

BBK Electronics began by manufacturing a range of CD, MP3, and DVD players, along with other household appliances, which appeared under a range of global brands. In 2004 Duan founded Oppo with CEO Tony Chen. Oppo built on Duan's experience in the video market by selling DVD and Blu-ray players, before moving into the smartphone market.

Vivo appeared a little later in 2009, and was founded by Duan and Vivo CEO Shen Wei. The first Vivo smartphones appeared in 2011 with a focus on ultra-slim form factors, while relying on celebrity endorsements to capitalize on the smartphone boom.

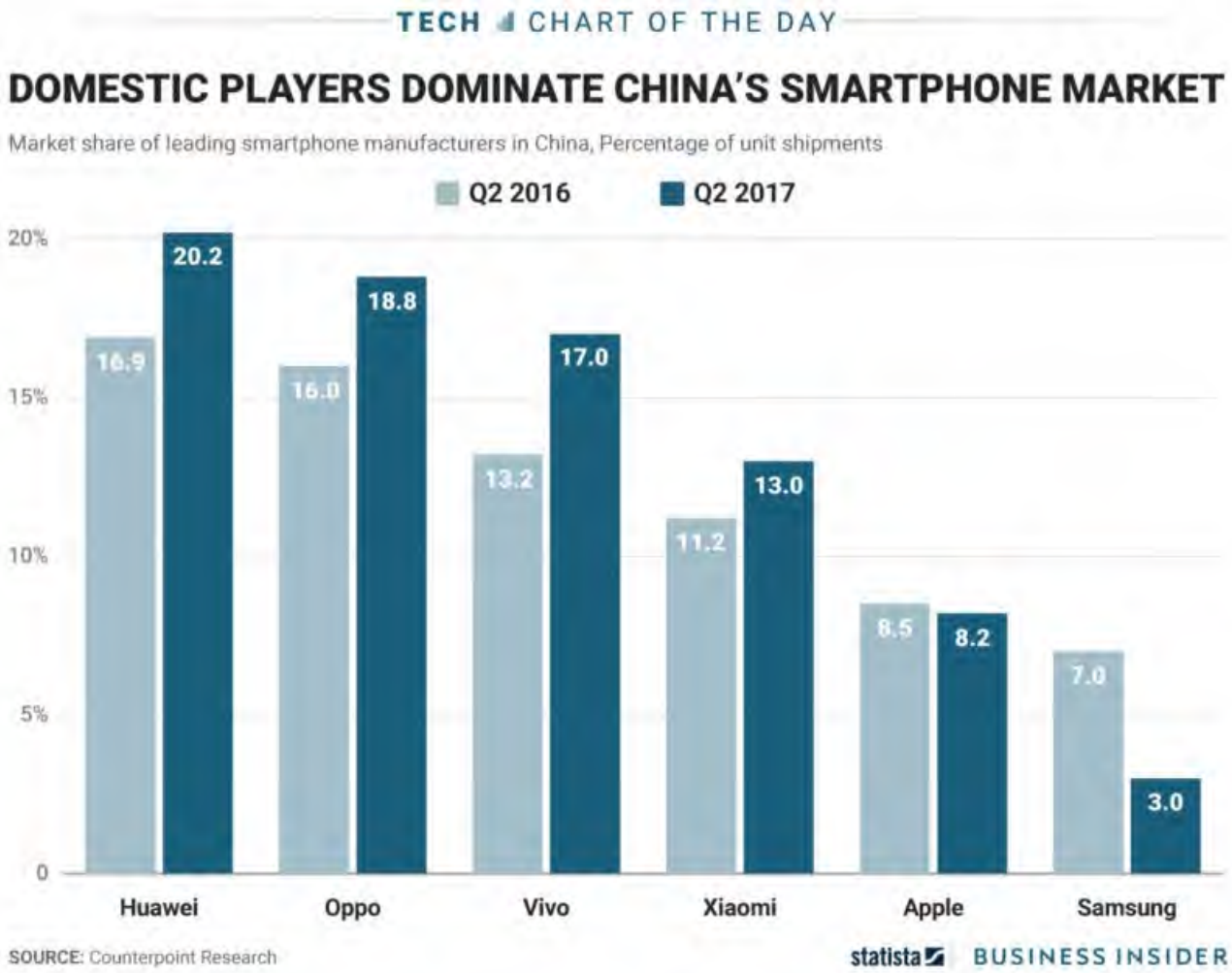
OnePlus, the BBK brand that Western customers might be most familiar with, wasn't started by Duan. It was founded by former Oppo vice president Pete Lau and co-founder Carl Pei in 2013, and is a subsidiary of Oppo. That still means it's owned by parent company BBK. OnePlus is arguably the most premium brand of

the three, however it takes a different approach to Oppo and Vivo's retail based business model. OnePlus primarily targets online sales via platforms like Amazon, which has helped BBK enter European and US markets.

Second or third place, depending on who you ask

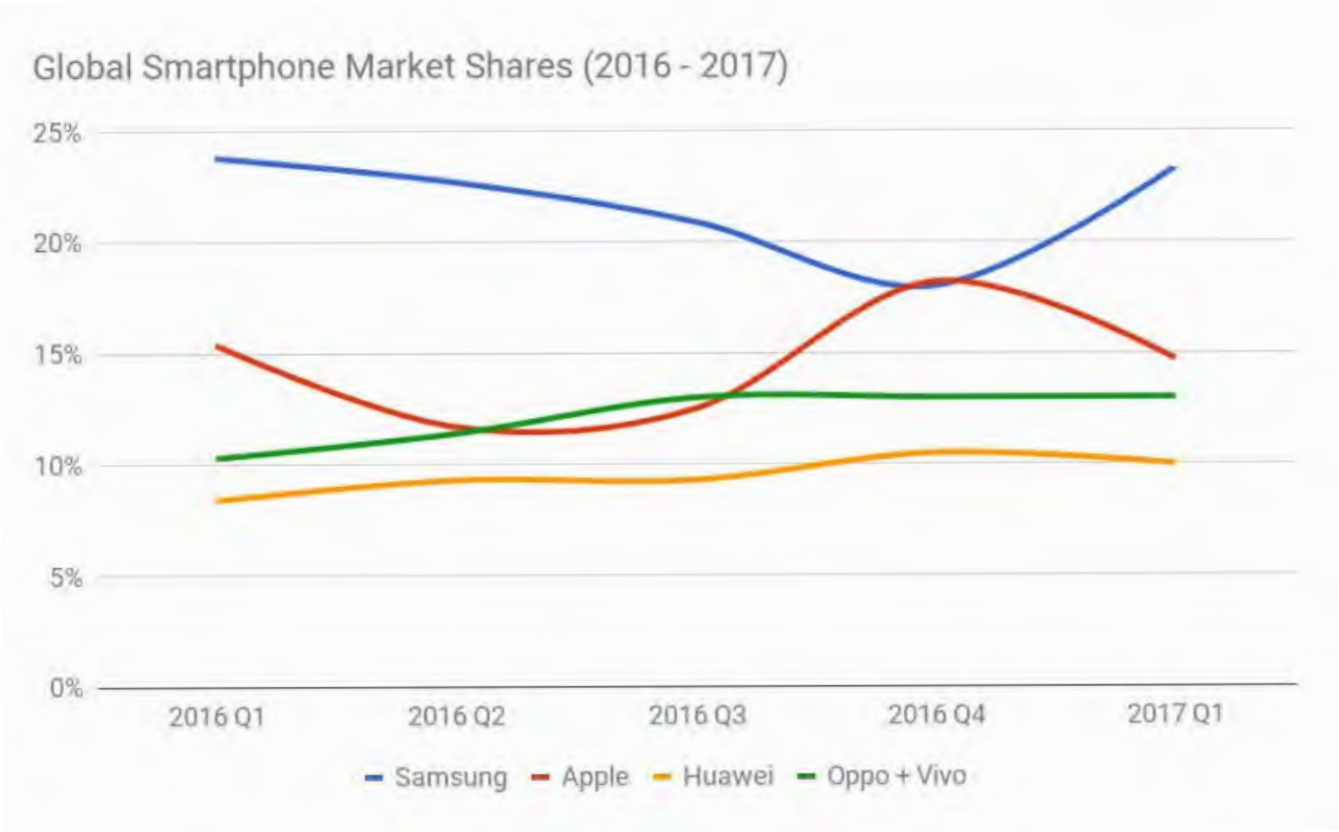
When it comes to smartphones, BBK Electronics is a big deal, even though most consumers have never heard of it. Oppo and Vivo have long been major players not just in the Chinese smartphone market, but internationally too.

In China, Oppo and Vivo have managed to surpass the growth rate of the once seemingly invincible Xiaomi by building a network of local stores, while its competitor focused on its efforts online. Apple and Samsung have struggled to keep pace with the cost competitive nature of China's homegrown mobile brands, including those in the BBK network. According to Counterpoint Research, Huawei is the biggest single brand with some 20.2% of China's market, but Oppo and Vivo are both very close behind on 18.8% and 17.0% respectively. Combined, BBK's smartphone brands have a comfortable lead with 35.8% of China's huge smartphone market.



Turning to the global outlook. In Q1 2017, Gartner research revealed that Oppo shipped around 30.9 million smartphones, with Vivo not far behind on 25.8 million. That's a combined total of 56.7 million. By comparison, Samsung shipped 78.6 million phones in the same quarter and Apple 51.9 million. BBK companies actually shipped more than Apple in Q1 2017, arguably putting them in second place, according to Gartner.

A similar report by IDC also paints a close picture, but with Apple retaining a small lead. According to its data, in Q1 2017 Samsung accounted for 23.3% of the global market, Apple on 14.7%, Huawei 10.0%, Oppo 7.5%, and Vivo 5.5%. Combined that would give BBK a market share of 13 percent, putting the company just behind Apple, but ahead of Huawei. OnePlus' market share isn't expected to account for even 1% of global sales, so it makes no meaningful difference to the rankings.



Market estimates always have some margin of error, but the data seems to suggest a close race for second between BBK and Apple. Throw Huawei into the mix and we're looking at three major companies all vying to close that gap on Samsung. That's a different picture than when looking at these brands individually, which sets the situation up as a simple first, second, and third ranking.

Looking forward

BBK Electronics isn't seemingly satisfied with just having a strong lead in China. The company recently overtook Samsung as the largest manufacturer in India, a key growth market. It also has a new phone brand named ikoo. This fourth smartphone sub-brand is looking to leverage experience in children's educational electronic toys to create the world's first education handset.

By spreading itself across multiple brands, BBK has managed to tailor its products to suit various market segments. The strategy has clearly paid off in China. Whether or not it will work in Western markets remains to be seen.

FEATURES NEWS

Tagged: OnePlus, Oppo, Vivo

Exhibit 14-EE

"Meet the 'Godfather' of China's Smartphone Industry"

SCMP.COM

South China Morning Post

Big Tech

Meet the ‘godfather’ of China’s smartphone industry

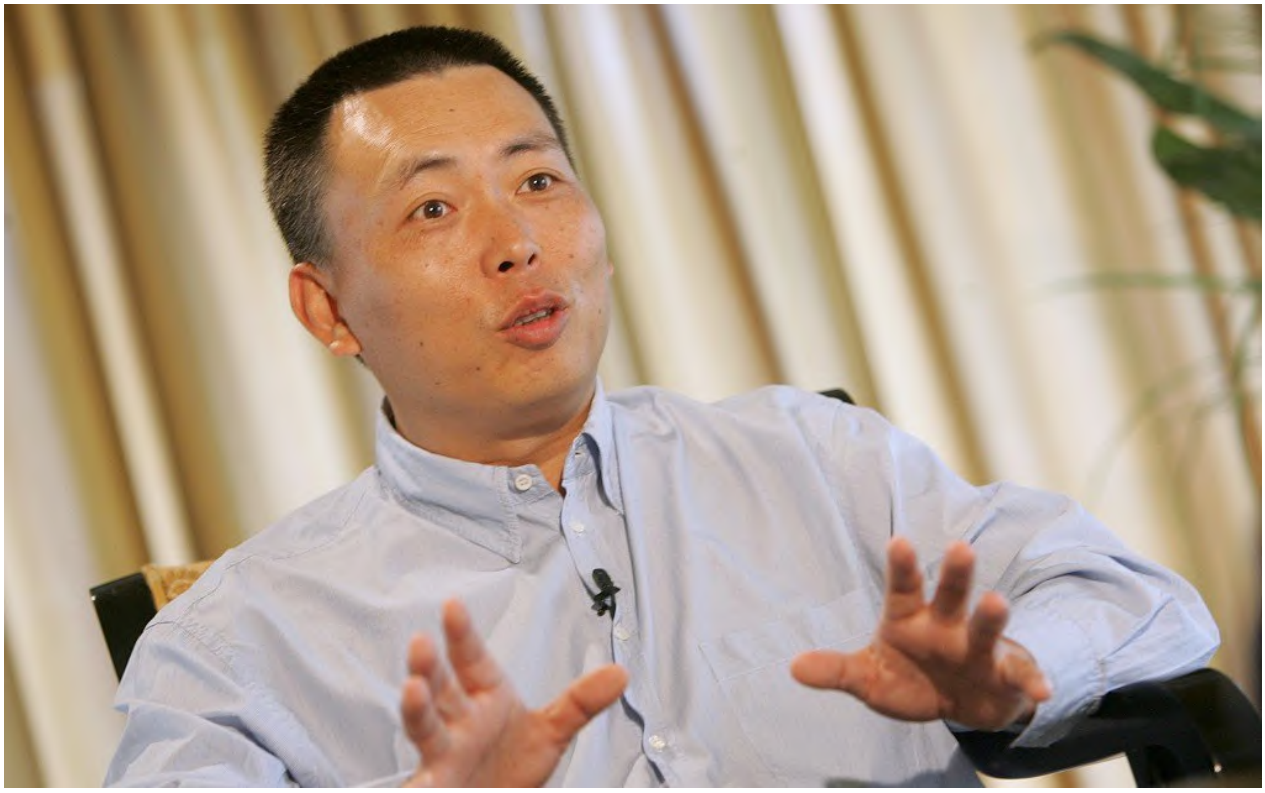
Duan Yongping is the founder and chairman of Dongguan-based BBK Electronics Corp

Privately held BBK is behind smartphone brands Oppo, Vivo, OnePlus and Realme

Topic | Smartphones

Li Tao

Published: 6:02am, 4 Feb, 2019



Over a span of about 10 years, Chinese smartphone brands have not only topped sales in their home market, but also outshone major foreign rivals in many emerging and developed economies.

The success of four of those brands – Oppo and Vivo as well as recently established OnePlus and Realme – can be directly attributed to the guiding hand and investment savvy of reclusive Chinese billionaire entrepreneur, investor and philanthropist Duan Yongping.

He is the founder and chairman of privately held BBK Electronics Corp, a 24-year-old company based in the southern coastal city of Dongguan that now runs one of the world’s largest and most sophisticated electronics supply chains behind the production of a range of smartphones for the global market.

Duan, who will turn 58 years old next month, is widely regarded as the “godfather” of the Chinese smartphone industry for developing two brands, Oppo and Vivo, as large global players competing against the likes of Samsung Electronics, Apple, LG Electronics and mainland rival Huawei Technologies. OnePlus and Realme, which are backed by BBK and other investors, look to be the next big Chinese brands to conquer international markets.

Attempts to reach Duan and BBK were unsuccessful. The Chinese billionaire, who was interviewed by Bloomberg in 2017, was identified last year as an early investor in Pinduoduo, China’s third largest e-commerce company, which was founded by his friend and protégé Colin Huang Zheng. Duan’s net worth was estimated at 10 billion yuan (US$1.5 billion), according to the 2018 *Hurun China Rich List.*

In September last year, Duan also had a well-publicised conversation with Chinese students at Stanford University in Palo Alto, California, where his family lives. Duan and wife Liu Xin, a former journalist, had set up their family’s Enlight Foundation to provide Chinese students undergraduate scholarships and graduate fellowships at the university’s School of Engineering.

Duan first made international headlines near the end of June 2006, when he agreed to pay a then-record amount of US$620,100 in a bidding on eBay to have a power lunch at a New York steakhouse with renowned billionaire investment guru Warren Buffett, the chairman and chief executive of Berkshire Hathaway.

~~Behind the rise of China’s smartphone brands lies growing unease over country’s tech gains~~

[1]

“I’ve learned so much from Warren Buffett and his investment philosophy. I want a chance to say thank you,” Duan said in a ~~*South China Morning Post*~~ *[2]* ~~report~~ [3] in July of that year. Apart from his wife, Duan brought six friends to that lunch, including Huang.

Born in March 1961 into a modest family in Nanchang, capital of Jiangxi province in southeast China, Duan in 1978 entered Zhejiang University in the eastern city of Hangzhou, where he majored in wireless electronics engineering.

After a short stint as a teacher at the adult education centre of the Beijing Radio Tube Factory, Duan pursued further studies at Beijing’s elite Renmin University of China, formerly known as People’s University, where he earned a master’s degree in economics in 1989.

Oppo was the world’s fifth largest smartphone supplier in 2018, according to data from Counterpoint Research. Photo: Reuters

That same year, he joined Zhongshan Yihua Group, located in the southern coastal province of Guangdong, to manage an ailing factory and turned it into a profitable business. He set up a unit that made cheap video game consoles, Subor Electronics Industry Corp, where he served as its chief executive.

Subor had much success in making education consoles, or learning machines, which were cheap copycats of Nintendo’s Famicom computers. That popular device, which was known as “Little Tyrant” in China and endorsed by Hong Kong martial arts superstar Jackie Chan at the time, helped Yihua achieve an annual profit of about 1 billion yuan (US$148 million) in 1995, compared with a loss of 2 million yuan when Duan joined the firm in 1989, according to a report by *Week in China* last year.

Despite that success, Duan had a public falling out with Yihua after his plan to spin off Subor and get a stake in the new company was rejected, the report said. He left Yihua in August 1995 and later that year, established electronics firm BBK, in which he had a controlling 70 per cent stake.

Vivo was the third biggest smartphone brand in China last year, according to research firm Canalys. Photo: Handout

Duan divided BBK’s business into three segments: education electronics, led by Huang Yihe; audiovisual, which made VCD and DVD players, under Chen Mingyong; and communications, which made mobile phones and cordless telephones, under Shen Wei. BBK had early success with its VCD and DVD players, becoming the leading vendor of those devices in China.

In 1999, Duan introduced a partnership programme that eventually led to the creation of independent business entities and reduction of his BBK stake to about 17 per cent. That led to Oppo Electronics Corp being founded in 2004 by Chen, while Vivo Communication Technology was formed by Shen in 2009. Pete Lau, the founder and chief executive of OnePlus, and Sky Li Bingzhong, founder of Realme, previously worked as vice-presidents at Oppo.

In his interview with Bloomberg, Duan said making mobile phones was not exactly his expertise, but reckoned his company could do well in the industry. That decision proved prescient, as sales of Chinese-brand Android smartphones took off when 3G and later 4G mobile networks were rolled out across the country.

~~Chinese smartphone brand Oppo doubles R&D investment to keep up with rivals ahead of 5G deployment~~

[4]

Demand for Chinese-brand mobile phones doubled each year between 2010 and 2012 during the period when 3G mobile services were being rolled out across the country, but gradually slowed down from 2013 ahead of the deployment of faster 4G services by the mainland’s three mobile network operators.

With the world’s biggest internet population and smartphone market, China had as many as 300 domestic mobile phone companies about three years ago. Cutthroat competition reduced that number to about 200 last year, as Chinese consumers bought fewer smartphones and the economy grew at a slower pace.

Only bet on the things you understand
Duan Yongping, chairman of BBK Electronics Corp

The larger, deep-pocketed Chinese smartphone suppliers have won a big chunk of the domestic market through aggressive promotions, advanced designs and features, and offering a wide array of models in a range of prices to entice both younger and affluent buyers.

Oppo and Vivo, respectively, were China’s second and third biggest smartphone suppliers in 2018, with a combined 40 per cent market share, according to estimates by research firm Canalys. They were behind market leader Huawei, but ahead of Xiaomi and Apple in a year when domestic smartphone shipments fell to 396 million units, compared with 459 million in 2017.

An employee tests the cameras of OnePlus smartphones at the company’s manufacturing facility in the southern coastal city of Dongguan, in Guangdong province. Photo: Bloomberg

In the global smartphone market last year, Oppo and Vivo took the fifth and six spots, respectively, with a combined 15 per cent share, according to data from Counterpoint Research. It said the top four-ranked vendors last year were Samsung, Apple, Huawei and Xiaomi.

Duan described the success of BBK along with sister brands Oppo and Vivo as no accident even if they were latecomers to the smartphone industry, according to a transcript of his talk with Stanford students last year. He attributed this to a focus on closely screening partners and suppliers, building “a great reputation”, making changes when something goes wrong and *benfen*, which loosely translates to integrity or honesty.

~~Vivo aims for high-end segment with premium, hi-tech handset sporting large dual displays~~
[5]

"In our early years, we often said our products provide good value at a cheap price," Duan said. "But over the years, I've learned that we were just making excuses for inferior products."

More than marketing and promotions, Duan said the goal was to focus on making a good products that meets users' requirements, whether in the low-end or high-end segment of the smartphone market.

~~China's OnePlus to launch first 5G smartphone in Europe with British carrier EE in 2019~~
[6]

Lau referred to *benfen* numerous times in an interview with the *Post* last year as the moral code that guides OnePlus, which he said helped the company gain the trust of consumers in the US and other overseas markets.

Duan, who emigrated to the US in 2002 to join his family, said he frowns on making speculative investments. "Only bet on the things you understand," he said. "Focus on understanding the business model and how the business makes money. Ninety-five per cent of investors focus on what the market will do. That's wrong."

Source URL: https://scmp.com/tech/big-tech/article/2184877/meet-godfather-chinas-smartphone-industry

Links
[1] https://www.scmp.com/tech/gear/article/2184131/behind-rise-chinas-smartphone-brands-lies-growing-unease-over-countrys
[2] https://www.scmp.com/article/556023/no-shortage-tips-buffett-lunch
[3] https://www.scmp.com/article/556023/no-shortage-tips-buffett-lunch
[4] https://www.scmp.com/tech/apps-social/article/2179613/chinese-smartphone-brand-oppo-doubles-rd-investment-keep-rivals
[5] https://www.scmp.com/tech/article/2177588/vivo-aims-high-end-segment-premium-hi-tech-handset-sporting-large-dual-displays
[6] https://www.scmp.com/tech/gear/article/2176545/chinas-oneplus-launch-first-5g-smartphone-europe-british-carrier-ee-2019

Exhibit 14-FF

"China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing"

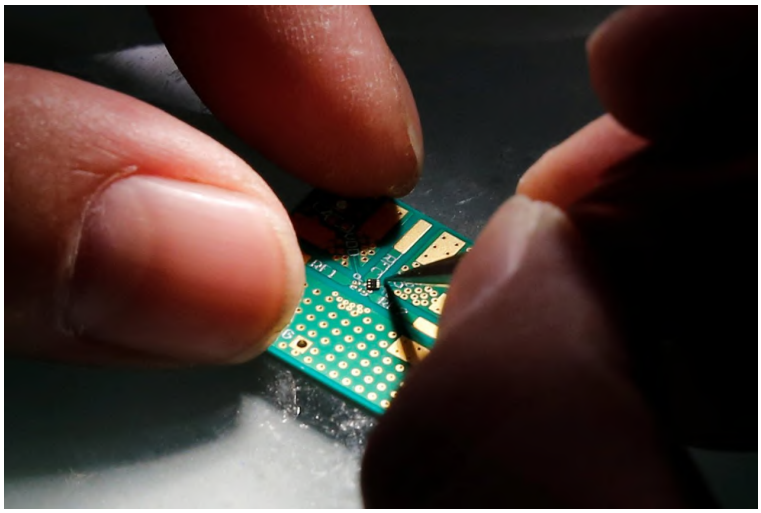
This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

https://www.wsj.com/articles/chinas-tsinghua-unigroup-to-build-30-billion-memory-chip-factory-in-nanjing-1484828235

TECH

China's Tsinghua Unigroup to Build $30 Billion Memory-Chip Factory in Nanjing

China is looking to diminish its dependence on U.S. chip manufacturers



A researcher plants a semiconductor on an interface board at a Tsinghua Unigroup research centre in Beijing. The company announced a $24 billion memory chip factory in Wuhan last March. PHOTO: KIM KYUNG-HOON/REUTERS

Updated Jan. 19, 2017 10:48 p.m. ET

BEIJING—China's flagship state-owned chip maker Tsinghua Unigroup said it plans to build a $30 billion memory-chip factory in Nanjing, its latest investment as China moves to diminish its dependence on U.S. chip manufacturers.

After several of its international chip deals were blocked by foreign governments, Tsinghua Unigroup has focused more on acquiring overseas talent and building its own plants.

This new planned plant comes after Tsinghua Unigroup announced a $24 billion memory chip factory in a different Chinese city, Wuhan, last March.

The U.S. is particularly wary about China's chip investments because semiconductors are one of the few sectors that the U.S. still manufactures competitively at home. Chips are the brains inside all computing devices and are an expensive technology that few companies can make.

Chinese officials say they need to be able to make the technology themselves to ensure national security. Beijing launched a $160 billion plan in 2014 to increase its share of domestically made

chips in its market from around 10% now to 70% over the next decade.

RELATED ARTICLES

- China's Tsinghua Unigroup Buys Small Stake in U.S. Chip Maker Lattice
- China's Tsinghua Unigroup to Build Memory Chip Factory
- China's Tsinghua Unigroup Plans to Buy Stakes in Taiwan Chip-Packaging Companies

An Obama administration advisory panel recommended this month that the U.S. tighten restrictions on Chinese chip investment in the U.S., citing national security reasons.

Tsinghua Unigroup said in a statement on its website that it will invest $30 billion in a factory in Nanjing to make storage chips, with monthly production capacity of 100,000 wafers. The technology, 3D-NAND and DRAM, is used in smartphones and other devices to store data.

In October 2015, Tsinghua Unigroup hired Charles Kau, former chairman of Taiwan's Inotera Memories Inc., as a vice chairman. Inotera is a joint-venture of Micron Technology Inc., a U.S. company that Tsinghua Unigroup unsuccessfully tried to acquire.

Other hires of Taiwan industry veterans followed. Tsinghua Unigroup said that it has executives including Shih-wei Sun, former chief executive of chip manufacturer United Microelectronics Corp. , James Shih, a former vice president of memory chip maker Nanya Technology Corp. , and Yuan Dih-wen, former senior executive of Taiwanese mobile chip designer MediaTek Inc.

—Eva Dou and Yang Jie

Copyright © 2019 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit https://www.djreprints.com.

Exhibit 14-GG

Tsinghua Holdings Co. Ltd.'s "Products and Technological Services" Webpage

Products and Technological Services

Globalization is one of the important development strategies of Tsinghua Holdings Co Ltd. Through multiple measures such as product exportation, technological services and international M&A, Tsinghua Holdings has built an international network and industrial layout across more than 150 countries and regions. It strives to improve its international reputation with top technologies, outstanding products and good services.

● Tsinghua Unigroup has acquired listed companies including Spreadtrum Communications Inc, RDA Microelectronics and Tongfang Guoxin Electronics Co Ltd. It also holds stock in New H3C, cooperates with Intel and participates in Powertech Technology Inc, Siliconware Precision Industries Co Ltd and ChipMOS Technology Inc. Its products are sold in nearly 100 countries and regions throughout the world and its clients include over 80 percent of the Global Fortune 500 companies. Moreover, it has established chip and Internet product R&D centers in a dozen countries, including the US and Finland.

● The security inspection products and services of Nuctech Company Limited are accessible in 150 countries and regions. The company has the world's largest market share of large container inspection systems. It provides security services for international and domestic events.

● The China National Knowledge Infrastructure, operated by Tongfang Knowledge Network, has built "CNKI digital library" with the largest amount of full-text information in the world, with users from different walks of life in China and over 40 other countries and regions. It draws on 76 percent of the globe's top 500 universities.

● Tus-Holdings Co Ltd cooperates with foreign countries such as Russia, Spain and South Korea to export TusPark's advanced concepts and development models. It has established two Sino-US cross-border incubation bases in Silicon Valley, which serve as bridges, linking good science and technology with innovative people. The company strives to be a super incubation platform for global innovation and entrepreneurship.

BUSINESS

Incubators

Hi-Tech Industries

Innovation Services

SPECIALS

● Tongfang Technovator's comprehensive, integrated service network for city energy conservation covers more than 60 countries and regions in the Middle East, North America and Europe.

● Global Safety Technology Co Ltd is China's first supplier of public safety emergency response solutions. Its products and services are exported to foreign countries such as Ecuador, Venezuela, Trinidad, and Tobago to build public security emergency command and control systems.

● The biochip related products and technologies of CapitialBio Corporation are accessible in over 30 countries and regions.

● Chengzhi Shareholding Co Ltd is a main supplier of L-glutamine and D-ribose in the global market, and its market share of D-ribose crystal exceeds 50 percent globally.

● Xuetangx.com, a subsidiary of MOOC-CN Education, has brought global high quality educational resources together, with a large number of users from more than 200 countries and regions.

● Tsinghua University Press has hundreds of print copyrights internationally, including in the US, UK, Japan, Singapore, South Korea and Thailand. Its English-version works and journals on science and technology sell well around the world.

● Huahuan Electronics Co Ltd focuses on information networks to develop various pieces of equipment for communication, transportation and access.

0

Tsinghua Holdings boosts technology and innovation along the Belt and Road

View All

Copyright © Tsinghua Holdings Co Ltd. All Rights Reserved. Presented by China Daily

Exhibit 14-HH

"Shenzhen Government Takes Control of China's Leading Chip Maker Tsinghua Unigroup"

SCMP.COM

South China Morning Post

China Business

Shenzhen government takes control of China's leading chip maker Tsinghua Unigroup

Tsinghua Unigroup is the third-largest smartphone chip maker in the world

Move part of a campaign to reduce corruption at university-owned enterprises

Topic | State-owned enterprises

Yujing Liu

Published: 9:15pm, 26 Oct, 2018

China's Tsinghua University will reduce its stake in the mainland's leading chip maker Tsinghua Unigroup amid a central government campaign to downsize the billions of dollars of corporate assets owned by public universities.

Tsinghua Holdings, which is owned by the public university, has agreed to transfer a 36 per cent stake in Unigroup to Shenzhen Investment Holdings, owned by the southern city's government agency overseeing state-owned assets, according to statements published by Unigroup's three Shenzhen-listed subsidiaries on Friday.

Tsinghua Holdings will retain a 15 per cent stake, according to the statements.

The campaign started to gain momentum since last June, when the Communist Party's anti-corruption watchdog found "high corruption risks" and "mismanagement problems" at school-affiliated enterprises run by 13 out of the 14 top universities it inspected. Tsinghua was the only school not named and shamed.

The party's reform policy formulation body released a guideline in May this year to call for tightened supervision and deeper reform of such enterprises, which are mostly in the hi-tech industry, as well as a clearer division between the schools' education and business operations.

Transferring company stakes to government-owned investment platforms is seen as one of the solutions that will also enhance the companies' competitiveness.

Tsinghua Unigroup shipped a total of 3.4 billion smartphone chips last year, making it the third largest mobile chip producer in the world, chief executive Zhao Weiguo said during a conference in August.

Tsinghua Holdings had previously signed agreements to transfer the stake to government-backed companies in the southern province of Hainan and Suzhou, Jiangsu province in eastern China in September. But they have since been terminated, according to the statements which did not provide the reasons behind its switch to Shenzhen.

Unisplendour Technology, a subsidiary suspended trading of its shares on Friday following the announcement.

https://www.scmp.com/tech/science-research/article/2161056/tsinghua-unigroup-president-calls-coexistence-foreign-chip
[1]

Source URL: https://scmp.com/business/china-business/article/2170440/shenzhen-government-takes-control-chinas-leading-chip-maker

Links
[1] https://www.scmp.com/tech/science-research/article/2161056/tsinghua-unigroup-president-calls-coexistence-foreign-chip

This article appeared in the South China Morning Post print edition as: Shenzhen to get 36pc stake in Tsinghua Unigroup

Exhibit 14-II

"Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology" by Interos Solutions, Inc.

Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology

APRIL 2018

Principal Author

Tara Beeny, Senior Business Analyst, Interos Solutions, Inc.

Subject Matter Experts

Jennifer Bisceglie, CEO, Interos Solutions, Inc.

Brent Wildasin, Managing Director, Interos Solutions, Inc.

Dean Cheng, Independent Contractor

Interos Solutions, Inc.

1725 Duke Street, Suite 510

Alexandria, VA 22314

PREPARED FOR THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Disclaimer: This research report was prepared at the request of the U.S.-China Economic and Security Review Commission to support its deliberations. Posting of the report to the Commission's website is intended to promote greater public understanding of the issues addressed by the Commission in its ongoing assessment of U.S.-China economic relations and their implications for U.S. security, as mandated by Public Law 106-398 and Public Law 113-291. However, it does not necessarily imply an endorsement by the Commission or any individual Commissioner of the views or conclusions expressed in this commissioned research report.

Table of Contents

Acronyms ..... **iii**

Executive Summary ..... **v**

Recommendations for a National SCRM Strategy vi

Embrace an Adaptive Supply Chain Risk Management (SCRM) Process vi

Centralize Federal ICT SCRM Efforts vii

Link Federal Regulations to Appropriations vii

Promote Supply Chain Transparency and Partnership with Industry vii

Craft Forward-Looking Policy viii

Chapter 1: U.S. Government ICT Supply Chains **1**

The Federal ICT Ecosystem 1

Quantifying the China Supplier Nexus 2

Tracing the China Supplier Nexus 3

Chapter 2: SCRM Laws, Regulations, and Other Requirements **6**

Federal Information Systems and NIST 6

National Security Systems and the CNSS 7

Executive Branch and SCRM 8

Congressional Action and SCRM 10

Federal Information Technology Acquisition Reform Act 10

Federal Information Security Modernization Act and Circular A-130 11

Cybersecurity Enhancement Act 12

Chapter 3: Supply Chain Analysis of Federal ICT Manufacturers **13**

Supplier Location 13

Supplier Financing and Influence 13

Supply Chain Risk Case Study: Corporate Intelligence-Sharing Agreements 16

Intel and IBM: (In)Security Partnerships 16

VMware Partnerships with Chinese SOEs and Kaspersky 17

Chapter 4: China's Political and Economic Agenda Is Behind the Supply Chain Security Dilemma **19**

Prioritizing Indigenous ICT Production 19

Raising Security Concerns 20

Extracting Concessions from Multinationals 21

Using Chinese Companies to Further State Goals 24

Targeting U.S. Government Contractors 27

Chapter 5: Closing Loopholes: Recommended SCRM Actions 29

Establishing Centralized Leadership for SCRM 29

Expanding the Wolf Provision 30

Promoting Supply Chain Transparency 31

Dodd-Frank Limitations Are Future SCRM Lessons 32

Utilizing Federal Acquisition Authorities 33

Chapter 6: Future Considerations 34

Conclusions 38

Scope Note 40

Methodology 40

Sources 41

Acknowledgments 42

List of Tables

Table 1
Federal IT Spending Ranked by Provider, FY 2015 1

Table 2
Examples of Federal ICT Suppliers Connected to Entities of Concern 14

Table 3
Foundational PRC Policies for Indigenous ICT Development 19

Table 4
Chinese Laws and Policies Related to ICT and National Security 22

List of Exhibits

Exhibit 1
China Supply for Seven Leading Federal IT Providers, 2012–2017 2

Exhibit 2
Annual Shipments by Suppliers to Cisco Systems, 2007–2017 4

Exhibit 3
U.S. Espionage Drives China's Nationalist IT Policy 20

Exhibit 4
Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm 36

Acronyms

3GPP	Third Generation Partnership Project
5G	fifth generation
CAS	Chinese Academy of Sciences
CETC	China Electronics Technology Group Corporation
CNCI	Comprehensive National Cybersecurity Initiative
CNITSEC	China Information Technology Evaluation Center
CNSS	Committee on National Security Systems
COTS	commercial off-the-shelf
CSF	Cybersecurity Framework (NIST)
DFARS	Defense Federal Acquisition Regulation Supplement
DHS	Department of Homeland Security
DoD	Department of Defense
DRC	Democratic Republic of the Congo
FDI	foreign direct investment
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FITARA	Federal Information Technology Acquisition Reform Act
GAO	Government Accountability Office
GSA	General Services Administration
HP	Hewlett-Packard
ICT	information and communications technology
IDC	International Data Corporation
IoT	Internet of Things
IP	intellectual property
IT	information technology
ITU	International Telecommunication Union
LCD	liquid crystal display
NIST	National Institute of Standards and Technology

NIST SP	NIST Special Publication
NSA	National Security Agency
NSS	national security systems
OECD	Organisation for Economic Co-operation and Development
OEM	original equipment manufacturer
OMB	Office of Management and Budget
PLA	People's Liberation Army
PRC	People's Republic of China
R&D	research and development
SCRM	supply chain risk management
SD	Specialized Disclosure (SEC form)
SEC	Securities and Exchange Commission
SOE	state-owned enterprise
TRM	Technical Reference Module
VA	Department of Veterans Affairs
ZTE	Zhongxing Telecommunications Corporation

Executive Summary

The U.S. government needs a national strategy for supply chain risk management (SCRM) of commercial supply chain vulnerabilities in U.S. federal information and communications technology (ICT), including procurement linked to the People's Republic of China (China or PRC). This strategy must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on responding to vulnerabilities, breaches, and other incidents after they have already damaged U.S. national security, economic competitiveness, or the privacy of U.S. citizens.

This study uses a comprehensive definition of "U.S. government ICT supply chains" that includes (1) primary suppliers, (2) tiers of suppliers that support prime suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. U.S. federal government ICT supply chains are multi-tiered, webbed relationships rather than singular or linear ones. The supply chain threat to U.S. national security stems from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by national governments or entities known to pose a potential supply chain or intelligence threat to the United States, including China. These products could be modified to (1) perform below expectations or fail, (2) facilitate state or corporate espionage, or (3) otherwise compromise the confidentiality, integrity, or availability of a federal information technology system.

Software supply chain attacks will become easier—and more prevalent—as developing technologies such as fifth generation (5G) mobile network technology and the Internet of Things (IoT) exponentially increase avenues for attack.[1] Gartner, an American information technology (IT) research and advisory firm, predicts that by 2021 there will be 25.1 billion IoT units installed,[2] and by 2020, IoT technology will be in 90 percent of new computer-enabled product designs.[3] This growth in IoT connectivity will have an important impact on the ICT SCRM challenge. Relevant to this report, increasing IoT installation will expand the attack surface of federal ICT networks while decreasing the time required to breach them, yet the time required to detect those breaches is not decreasing. The responsibility of both the public and private sectors in increasing their approach to risk awareness and management in the commercial technology supply chain cannot be overstated.

China did not emerge as a key node on the global ICT supply chain by chance. The Chinese government considers the ICT sector a "strategic sector" in which it has invested significant state capital and influence on behalf of state-owned ICT enterprises. China has long-standing policies encouraging ICT manufacturing and development. These policies offer incentives for foreign companies to produce ICT in China, while at the same time pursuing opportunities to obtain key intellectual property and technology from those companies with the ultimate goal of indigenizing these technologies. Since 2013, China has accelerated its efforts at indigenous production and independence. This shift has made for a more restrictive environment for companies doing business in China, extracting concessions from large multinationals in exchange for market access. At the same time, China has expanded its efforts to obtain economic advantage by pursuing knowledge of key technologies through corporate acquisitions and by using the economic power of Chinese companies as tools of the state. The PRC government justifies these policies in terms of ensuring China's own national security, but China's policies related to prioritizing indigenous production, extracting concessions from multinationals, using Chinese companies as state tools, and targeting U.S. federal networks and the networks of federal contractors have heightened risks to the U.S. ICT supply chain, and to U.S. national and economic security. New policies requiring companies to surrender source code, store data on servers based in China, invest in Chinese companies, and allow the Chinese government to conduct security audits on their products open federal ICT providers—and the federal ICT networks they supply—to Chinese

1 The Internet of Things refers to a system of interrelated computing devices, mechanical and digital machines, objects, and living beings equipped with network connectivity that enables them to connect and exchange data.

2 Peter Middleton et al., "Forecast: Internet of Things–Endpoints and Associated Services, Worldwide, 2017," Gartner, Inc., December 21, 2017, https://www.gartner.com/doc/3840665/forecast-internet-things--endpoints.

3 Benoit J. Lheureux et al., "Predicts 2018: Expanding Internet of Things Scale Will Drive Project Failures and ROI Focus," Gartner, Inc., November 28, 2017, https://www.gartner.com/doc/3833669/predicts--expanding-internet-things.

cyberespionage efforts and intellectual property theft. China also continues to target U.S. government contractors and other private sector entities as part of its efforts to gain economic advantage and pursue other state goals.

RECOMMENDATIONS FOR A NATIONAL SCRM STRATEGY

Effective SCRM is the ability to anticipate future developments in supply chains, identity potential threats to supply chains, develop threat profiles, and mitigate or address future threats to the supply chain. Federal government laws and policies do not address SCRM comprehensively. The evolution of global production and manufacturing of ICT products and the nature of federal ICT modernization efforts means new products entering the federal information systems and national security systems have increasingly complex and globalized supply chains, many of which originate with commercial suppliers sourcing from China. It is unlikely that political or economic shifts will cause global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. How, then, should the U.S. government manage risks associated with Chinese-made products and services and the participation of Chinese companies in its ICT supply chains? Federal ICT supply chain risks can be best managed by embracing an adaptive SCRM process, centralizing the leadership of federal ICT SCRM efforts, linking federal regulations to appropriations, promoting supply chain transparency, and crafting forward-looking policies.

EMBRACE AN ADAPTIVE SUPPLY CHAIN RISK MANAGEMENT (SCRM) PROCESS

Federal ICT modernization efforts have increased reliance on the private sector and commercial off-the-shelf (COTS) products. These new products have increasingly complex, globalized, and dynamic supply chains, many of which include commercial suppliers that source from China at multiple points within a single supply chain. These supply chains change over time as companies develop new technologies and partner with new suppliers, and effective SCRM policies must be able to adapt as well. Nefarious actors linked to China have targeted the networks of private sector entities and private sector government contractors in order to obtain sensitive government information and to exploit vulnerabilities within federal information systems. Thus, weaknesses in the networks of industry partners pose a threat to the U.S. government and U.S. national security.

Defending against supply chain attacks by nefarious actors linked to China requires communication and collaboration with private sector actors. The National Institute of Standards and Technology (NIST) has been effective in partnering with the private sector to produce high-quality, implementable standards to improve supply chain security and cybersecurity of ICT systems, including the widely adopted NIST Cybersecurity Framework. Although NIST has been effective in these efforts, supply chain controls developed by NIST apply only to "high-impact" federal information systems.[4] Future work by NIST could include expanding supply chain standards to a broader range of federal information systems, including systems operated by private sector contractors.

Partnering with industry also means learning from experience with efforts such as the Bush-era Comprehensive National Cybersecurity Initiative (CNCI). The CNCI's effectiveness was limited by the classified nature of its deliberations and decisions, which prevented the U.S. Department of State and the National Cyber Security Center from engaging with outside organizations, including the private sector. Policymakers must empower rather than hinder the efforts of successful collaborative entities such as NIST and keep as much discussion of the supply chain threat as possible in the unclassified public sphere. These steps will ensure that new SCRM policies can be adaptive, be collaborative, and achieve buy-in from all relevant parties.

4 FIPS Publication 199 categorizes an information system as high impact as when "the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals." In this case, "A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." If any of the information on a federal information system is classified as high impact with respect to confidentiality, integrity, or availability, then the entire information system is considered high impact. See National Institute of Standards and Technology, *FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, February 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

CENTRALIZE FEDERAL ICT SCRM EFFORTS

The U.S. government lacks a consistent, holistic SCRM approach. Additionally, most federal SCRM-related intelligence gathering activities are people based rather than technology based. This makes it difficult for federal SCRM programs to address the global threat comprehensively, or to scale as demand increases. The conflicting and confusing laws and regulations result in loopholes, duplication of effort, and inconsistently applied policies. Congress and the Executive Branch should encourage information sharing and the consolidation of federal SCRM leadership to optimize collection and dissemination efforts. Centralized leadership for SCRM would need to be resourced and staffed appropriately and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering the federal IT network.[5] The Office of Management and Budget (OMB) could, through modifications to Circular A-130,[6] assign centralized SCRM authority to the General Services Administration (GSA), the U.S. Department of Homeland Security (DHS), or another federal agency. This SCRM center would provide comprehensive and authoritative data and continuous monitoring, which would reduce the need for agency-specific SCRM and allow agencies to focus their efforts on particular configurations and implementation situations; how agencies use technology directly relates to how they apply risk mitigations. Last, such an office would need to function in the unclassified world, while at the same time having direct connections and reach-back authority into the classified environment to ensure it remains in alignment with known threats. As illustrated by the experience of the CNCI, the relationship should not be reversed and come entirely under classified control.

LINK FEDERAL REGULATIONS TO APPROPRIATIONS

Along with modifications to policy—such as Circular A-130—Congress should tie policy revisions to a funding strategy that ensures federal agencies take action in ways that are auditable. One recommendation is to expand the Wolf Provision, or Section 515 of the Consolidated and Further Continuing Appropriations Act, to apply to all federal agencies and entities. A near-term opportunity is to tie the SCRM requirements of this regulation to agency funding for the Modernizing Government Technology Act of 2017 in ways that require a SCRM program review for new ICT investments and modernization efforts. One improvement to the provision would be to require agencies to annually present (1) information about their established SCRM program, (2) the activities that have taken place within that program, and (3) the mitigations used. These annual reports will help build a best practices library for all federal government entities, increasing information sharing and awareness of evolving risks. The current reporting is compliance oriented and does nothing to share information or increase the security posture of federal ICT networks.

PROMOTE SUPPLY CHAIN TRANSPARENCY AND PARTNERSHIP WITH INDUSTRY

Supply chain transparency increases the security of the federal ICT supply chain by enabling the federal government to source responsibly and securely, and by improving the government's ability to respond to, and reduce the impact of, cybersecurity incidents in an environment where supply chain attacks are ongoing. Directly in relation to the impact on national security, the federal government should promote the public listing—or at least the disclosure to the government customer—of federal ICT providers and primary or tier-one suppliers in line with actions already taken by companies such as Dell, Hewlett-Packard (HP), and Microsoft as part of their corporate responsibility efforts. The government should also push for transparency on the part of all suppliers within its own supply chain according to the level of risk management rigor required (not all programs and suppliers present the same level of risk and therefore this level of transparency may not be needed). This information does not always need to be publicly released, though audit measures should be in place to ensure the transparency exists. In taking these measures, policymakers should learn from previous supply chain transparency efforts, such as Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which required some companies to document their suppliers of "conflict minerals" in order to decrease violence in the Democratic Republic of the Congo (DRC) by limiting U.S. procurement from actors fueling conflict in the DRC. By partnering with industry and sharing information, the government customers and industry will have increased awareness of risks present in multi-tiered supplier relationships, as well as potentially effective mitigations that are already in place.

5 A value-added reseller is a company that purchases products from a vendor (generally at a discount); adds additional features, services, or support to the existing product; and then resells the product as an "integrated" or "turn-key" solution.

6 Circular A-130 provides policy guidance to federal agencies on the governance of IT resources, including governance, acquisitions, records management, open data, workforce, security, and privacy. The circular established minimum requirements for federal information security and privacy programs and assigns responsibilities for the security of those systems.

CRAFT FORWARD-LOOKING POLICY

Increasingly, any ICT component's physical structure pales in importance compared with the firmware and software operating within in it. Future risks will involve software, cloud-based infrastructures, and hyper-converged products rather than hardware. A vendor's, supplier's, or manufacturer's business alliances, investment sources, and joint research and development (R&D) efforts are also sources of risk that are not always covered in traditional SCRM. Identifying these risks and addressing them creatively as part of the adaptive approach to supply chain risk management will be important to the success of federal policy efforts.

Chapter 1: U.S. Government ICT Supply Chains

The OMB's 2017 budget proposal allocated $89.9 billion for IT in fiscal year (FY) 2017.[7] In 2016, International Data Corporation's (IDC's) Government Insights and FedScoop jointly released a study claiming that the U.S. federal ICT market is "the largest single vertical market for IT in the U.S. today, representing about 8.6 percent of all IT spending in the U.S., followed by the banking industry, at 7.6 percent."[8] FedScoop released two rankings in connection with the study: the "Top 25 Enterprise IT Providers to Government" and the "Federal IT Top 100." The top 10 companies on each list are shown in **Table 1**. Despite the size of the U.S. federal ICT market, IDC's research indicates that over 50 percent of federal IT spending goes to the top 10 suppliers on the lists, making their supply chains worthy of particular scrutiny for potential risk access points. It should be noted that Intel ranks at number 11 on the "Top 25 Enterprise IT Providers to Government" list, and also serves as a provider of primary technology components to many of the other companies in the top 10, thus its inclusion in this report.

THE FEDERAL ICT ECOSYSTEM

IDC and FedScoop's "Top 25 Enterprise IT Providers to Government" list ranks major enterprise IT companies by their estimated government-only sales.[9] The list includes the largest manufacturers of federal ICT equipment, including leading providers of COTS products, such as HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.

The second list, the "Federal IT Top 100," ranks integrators and solution providers on the basis of revenue from the sale of IT products and services to federal agencies.[10] This list includes key players in government ICT contracting—firms that provide, manage, and, in some cases, modify the products produced by firms on the enterprise providers list.

Table 1
Federal IT Spending Ranked by Provider, FY 2015

Ranking	Top 25 Enterprise IT Providers to Government	Federal IT Top 100
1	Hewlett-Packard	Lockheed Martin
2	IBM	National Security Technologies
3	Jeppesen Sanderson (Division of Boeing)	Leidos, Inc.
4	Dell	Battelle Memorial Institute
5	Computer Sciences Corporation[1]	Northrop Grumman
6	Cisco	SAIC
7	Boeing	UChicago Argonne
8	Deloitte Consulting	Harris
9	Unisys	Consolidated Nuclear Security
10	Microsoft	Raytheon

Note: These rankings are based on actual revenues generated from the sale of IT products and services during the federal government's FY 2015, not multiyear contract awards. IDC has removed non-IT spending that is often included in IT contracts (such as management, consulting, and energy costs).

1. On April 3, 2017, Computer Sciences Corporation merged with Hewlett-Packard Enterprise Services to create DXC Technology.

Sources: IDC Government Insights and FedScoop.

7 Phil Goldstein, "2017 Budget Boosts IT Spending to $89.9 Billion, Expands U.S. Digital Service," *FedTech*, February 9, 2016, https://fedtechmagazine.com/article/2016/02/2017-budget-boosts-it-spending-899-billion-expands-us-digital-service.

8 Wyatt Kash, "New Top 100 Rankings Reveals Which Firms Earn the Most from Federal IT Spending," FedScoop, June 24, 2016, https://www.fedscoop.com/federal-it-top-100-report-on-government-it-spending/.

9 "Top 25 Enterprise IT Providers to Government," FedScoop, August 30, 2017, https://www.fedscoop.com/federal-it-top-25/federal-it-top-25-full-list/.

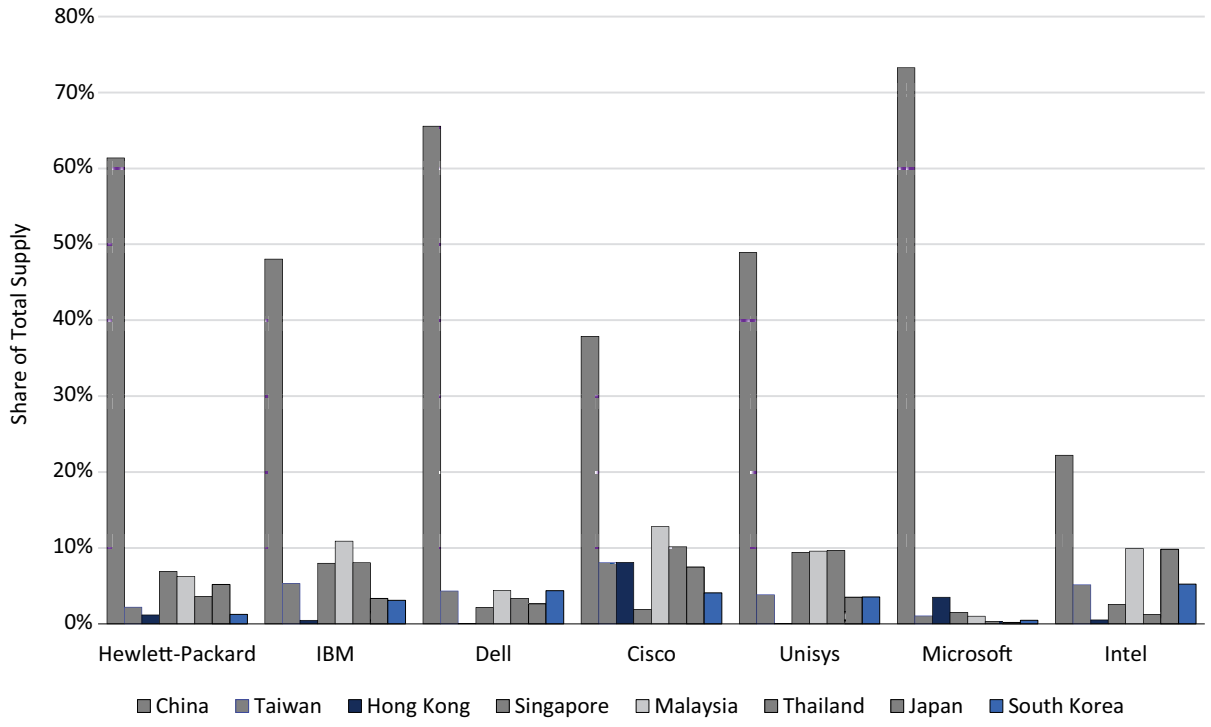
10 "Federal IT Top 100 – Federally Focused IT Providers," FedScoop, August 30, 2017, https://www.fedscoop.com/federal-it-top-100/full-list/.

QUANTIFYING THE CHINA SUPPLIER NEXUS

In breaking down the supply chain implications for top companies on the enterprise providers list, this report focuses on seven manufacturers: HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel. These seven companies are some of the top IT providers to the U.S. government that are primarily IT manufacturers, and for which sufficient open source supply chain data exist. The nature of available open source information can make it difficult to separate data from a parent company from those of its subsidiaries; for example, data for Jeppesen Sanderson are tied to data for Boeing. The available data sets for Computer Sciences Corporation and Deloitte Consulting are too small to support firm conclusions. Focusing on these seven major IT manufacturers can illustrate the trends and challenges of supply chain risk analysis for commercial IT products. This is not to say these are the only companies with potential challenges in their supply chains, and it should be noted that none of these companies were approached as part of this report. Although each company conducts some level of due diligence on its supplier base, the complete records are not publicly available. Additional analysis of the aforementioned Jeppesen Sanderson, DXC Technology, and Deloitte, as well as other top federal enterprise IT providers such as AT&T, Abacus Technology, and Amazon Web Services, would provide a more comprehensive understanding of the federal ICT ecosystem.

Exhibit 1 provides transactional data culled from publicly available information for HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel. The graph shows the percentage of shipments originating in various countries between September 8, 2012, and September 7, 2017, for each company and its subsidiaries. These data provide a broader picture than U.S. trade data, as they include import and export data for other countries as well, including Bolivia, Chile, China, Colombia, Costa Rica, Ecuador, Mexico, Panama, Paraguay, Peru, Uruguay, and Venezuela. As the chart shows, China is the overwhelming source of products for these manufacturers. An average of 51 percent of shipments to these seven commercial IT manufacturers originate in China. Microsoft has the largest share of shipments originating in China, at 73 percent.

Exhibit 1
China Supply for Seven Leading Federal IT Providers, 2012–2017



Source: Panjiva.

Over 95 percent of all commercial electronics components and IT systems supporting U.S. federal IT networks are COTS, and China's role in this global supply network is significant. The supply chain for commercial IT is a global enterprise dominated by suppliers in East Asia.[11] In addition to Chinese firms, many companies headquartered in Taiwan and Singapore base their manufacturing operations primarily in China. China assembles most of the world's consumer and commercial electronic devices, produces parts such as flash cards, and dominates the world in volume of IT industrial capacity. A recent report from the Government Accountability Office (GAO) notes that China is the largest importer and exporter of IT hardware globally, as well as a key manufacturing location of workstations, notebook computers, routers and switches, fiber optic cabling, and printers.[12]

TRACING THE CHINA SUPPLIER NEXUS

Changing market dynamics and the increasing complexity of the commercial ICT supply chain have created additional challenges for supply chain risk management. During the transformation from raw materials to finished products, ICT components can transit several national borders. As one study showed, the elements that are eventually incorporated into an Apple iPod may be sourced from suppliers in the United States, Japan, Taiwan, and South Korea and assembled in plants in China run by Taiwanese corporations.[13] Assembled products may then pass through distribution centers in South and Central America to retail locations across the United States. This circuitous production path complicates the accuracy of trade data, as recent studies have shown, as well as the process of supplier management and supply chain tracing. Not only is it difficult to calculate the value added during each manufacturing step, but it is difficult to assess the risks associated with each new component supplier and contract manufacturer in the supply chain.

In addition, it is increasingly difficult for analysts to independently understand the nature of ICT supply chains. As little as 5–10 years ago, data from transactional information sources could trace ICT shipments from component producers in mainland China and Taiwan to manufacturing centers in North and South America. However, as the emerging middle class in China consumed more ICT technologies, China, Hong Kong, and Taiwan became favored locations for ICT firms' production facilities.[14] In China especially, government subsidies and policies requiring relocation in exchange for market access further encouraged multinationals to establish subsidiaries and joint ventures on the mainland. The establishment of multinational subsidiaries in East Asia has made independent open source supply chain analysis more difficult. Often the biggest supplier for many U.S. ICT companies, especially the larger ones, is their own East Asian subsidiary. For example, the largest supplier for Intel-Mexico, Intel-Colombia, and Intel-USA is Intel-Shanghai. Identifying the secondary and tertiary suppliers that contribute products and value early in the supply chain can be challenging due to the lack of transparent documentation and constantly changing business relationships. **Exhibit 2** provides an example of this phenomenon.

11 Danny Lam and David Jimenez, "US' IT Supply Chain Vulnerable to Chinese, Russian Threats," *The Hill*, July 9, 2017, http://thehill.com/blogs/pundits-blog/technology/341177-us-it-supply-chain-vulnerable-to-chinese-russian-threats.

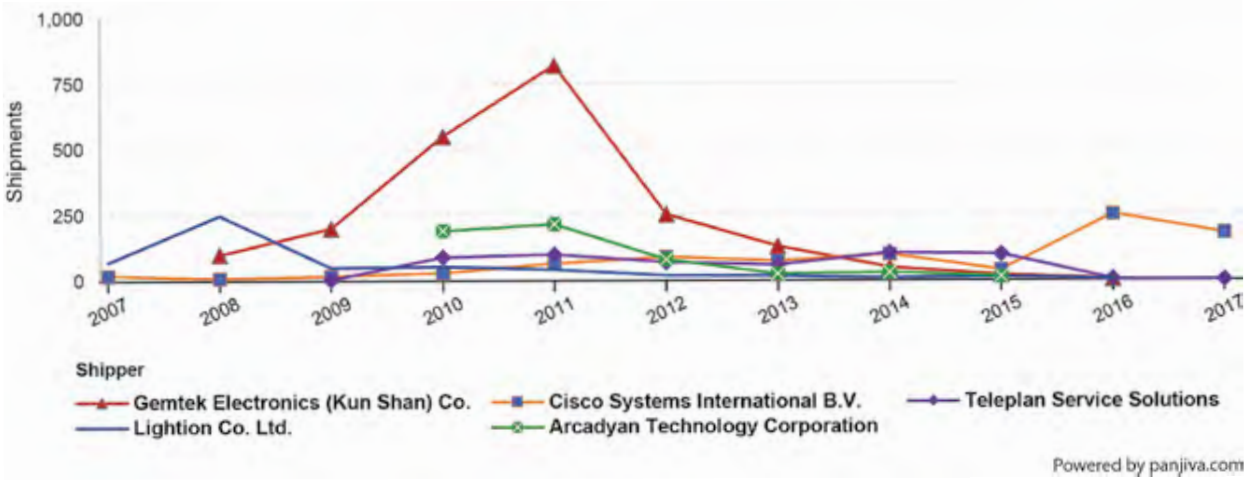
12 U.S. Government Accountability Office, "State Department Telecommunications: Information on Vendors and Cyber-Threat Nations" (GAO-17-688R State Department Telecommunications, July 27, 2017), https://www.gao.gov/assets/690/686197.pdf.

13 Greg Linden, Kenneth L. Kraemer, and Jason Dedrick, "Who Captures Value in a Global Innovation Network? The Case of Apple's iPod," *Communications of the ACM* 52, no. 3 (March 2009): 140–44, http://pcic.merage.uci.edu/papers/2008/whocapturesvalue.pdf.

14 Organisation for Economic Co-operation and Development (OECD), *OECD Science, Technology and Innovation Outlook 2016* (Paris: OECD Publishing, 2016), http://dx.doi.org/10.1787/sti_in_outlook-2016-en.

Exhibit 2

Annual Shipments by Suppliers to Cisco Systems, 2007–2017



Source: Panjiva.

Exhibit 2 shows the year-to-year shift in Cisco's U.S. import registered supplier data, as shipments from Gemtek Electronics (Kun Shan) Co. Ltd. (China), Arcadyan Technology Corporation (Taiwan), and Lightion Co. Ltd. (Hong Kong) gradually disappear from the data set and are replaced by shipments from Cisco Systems International B.V., a subsidiary based in the Netherlands that appears to manage Cisco's international shipments. This trend effectively masks the deeper levels of Cisco's supply chain, making it less clear which East Asian companies are serving as third- and fourth-tier suppliers.

A similar pattern is evident among the other top enterprise IT providers to the federal government. HP's top two suppliers of China-origin goods are its own subsidiaries in Singapore and Mexico. Unisys's primary shipper of China-origin products is Unisys C O Exel, which began shipping from China to Unisys subsidiaries in Mexico and Colombia around 2012. For Intel, Microsoft, Cisco, Boeing, and IBM, the top supplier of China-origin items is the company itself.

The practice of sourcing primarily from foreign subsidiaries can make it more difficult to determine the primary component suppliers in a supply chain, and this lack of transparency is itself an added source of risk. This is because for SCRM, both the location of the production and the entity in control of that production are important factors in assessing risk. Risks associated with location and control of production exist along a spectrum, and can be aggravated or mitigated by other factors. Production by a Chinese state-owned enterprise (SOE) based in China presents greater risk to the federal ICT supply chain than production by a Singaporean firm based in China, yet both present more risk than a Singaporean firm based in Singapore. This is because production based in sensitive countries or in countries known for counterfeiting and intellectual property (IP) violations poses heightened risk regardless of who does the manufacturing. Due to reliance on foreign legal, political, and financial systems and labor markets, as well as the infrastructure of a foreign nation, foreign subsidiaries may be at greater risk of penetration by nefarious actors than domestic subsidiaries and a company's recourse in the event of penetration may be more limited. In China in particular, companies involved in trade disputes or corporate litigation can encounter difficulties obtaining records or serving subpoenas that would allow prosecution, and must prove they have taken steps to properly safeguard trade secrets in order to successfully sue.[15]

15 Del Quentin Wilber, "Stealing White: How a Corporate Spy Swiped Plans for DuPont's Billion-Dollar Color Formula," Bloomberg, February 4, 2016, https://www.bloomberg.com/features/2016-stealing-dupont-white/.

The entity in control of production also factors into the analysis. A parent company has most control over location security, staff hiring, manufacturing, and quality control practices at domestic subsidiaries. Depending on a company's corporate culture and internal controls, that same company may have more control at a foreign subsidiary than it would at a foreign third-party manufacturer. Apple, for instance, has instituted strict controls at its production sites in China in an effort to secure its supply chain and protect its IP.[16] However, the foreign subsidiary may still be subject to foreign regulations or influence in ways that increase risk related to a company and its products.

16 William Turton, "Leaked Recording: Inside Apple's Global War on Leakers," *The Outline*, June 20, 2017, https://theoutline.com/post/1766/leaked-recording-inside-apple-s-global-war-on-leakers.

Chapter 2: SCRM Laws, Regulations, and Other Requirements

Supply chain risk management is an important component of a comprehensive cybersecurity mission, but it also has a role in market research, acquisitions, and procurement, as well as broader programmatic activities such as program lifecycle planning. A challenge facing federal SCRM efforts is that federal government laws and policies do not address risk management comprehensively. Rather, as the following sections will show, SCRM of federal ICT systems has been divided in multiple ways—among federal information systems and other initiatives designed to protect critical infrastructure or high-value assets and among national security systems (NSS) as a subset of federal information systems.

FEDERAL INFORMATION SYSTEMS AND NIST

The OMB has purview over federal information systems "used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency."[17] NIST creates standards and guidelines for these systems. NIST is not a regulatory agency; rather, it develops security standards and guidelines through a comprehensive public review process. For many products, this process involves three cycles of public vetting, during which comments on draft publications are solicited from individuals and organizations in the public and private sectors.[18] NIST's outreach efforts encourage feedback and discussion, particularly from owners, operators, and administrators of the information systems for which NIST sets standards. This process aims to ensure that the guidelines are both technically correct and implementable.

In 2002, Congress passed the Federal Information Security Management Act (FISMA), which required NIST to develop security standards and guidelines to protect federal information systems and allowed the OMB to make NIST standards compulsory and binding.[19] NIST's FISMA Implementation Project was established in 2003 to produce the required security standards and guidelines for federal information systems; its publications include Federal Information Processing Standards (FIPS) 199, FIPS 200, and the NIST Special Publications (NIST SP) 800 series.

Neither FIPS 199 (2004) nor FIPS 200 (2006) mention supply chain issues. FIPS 199 focuses on categorization, creating the requirement to rate information systems as low, moderate, or high impact in terms of confidentiality, integrity, and availability.[20] FIPS 200 sets some minimum security requirements in the areas of access control, awareness and training, configuration management, media protection, personnel security, resource allocation, and licensing policy, among others. FIPS 200 also introduced the concept that risk management includes "continuous" or "ongoing" monitoring of the security state of the information system.[21]

The FIPS 199 categorizations and policies are used to determine which systems are subject to enhanced cybersecurity measures and SCRM requirements, but the FIPS standards do not require SCRM of those systems, or specify the scope or extent of supplier due diligence that should be used in evaluating products, services, or suppliers of those systems. The FIPS 200 controls are designed to mitigate threats posed by individuals who are improperly trained or credentialed, and to avoid resource management errors that may result in an improperly disposed hard drive or an improperly used or licensed software program. They are not designed to mitigate risk posed by ICT products that may have been compromised during the manufacturing, programming, or deployment process. This separation is intentional. Supplemental information released with FIPS 200 in March 2006 explained that during the review

17 "Circular No. A-130: Managing Information as a Strategic Resource," Office of Management and Budget, July 28, 2016, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf.

18 "FAQs: General Questions, National Institute of Standards and Technology," Computer Security Resource Center, updated October 18, 2017, http://csrc.nist.gov/groups/SMA/fisma/faqs.html.

19 This means that standards created under the authority of Sections 20(a) and 20(b) of the National Institute of Standards and Technology Act 15 U.S.C. 278g–3(a) were mandatory.

20 National Institute of Standards and Technology, *FIPS PUB 199*.

21 National Institute of Standards and Technology, *FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, March 2006), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf.

process NIST had received comments suggesting "additions and changes to the standard concerning risk management procedures, audit controls, baseline security controls, and risks introduced by new technologies," all of which could be considered SCRM-related. NIST's response to this comment indicated that these elements were best addressed in forthcoming NIST SP 800-53, and ultimately aggregated from across all NIST SPs in SP 800-161, rather than updated in the FIPS 199 and 200 series.[22] The result of this decision is that while FIPS 199 and 200 controls are legally mandated, the SCRM-related controls in NIST SPs remain merely guidance. A stronger legal or regulatory requirement relating to SCRM could help bridge this gap. That said, it is not—nor should it be—the role of NIST to enforce stronger legal or regulatory requirements, as this would severely diminish NIST's value as convening entity.

NATIONAL SECURITY SYSTEMS AND THE CNSS

Policies for NSS are controlled by the Committee on National Security Systems (CNSS). The CNSS is an interagency body chaired by the Department of Defense (DoD) and the U.S. military, with membership from the intelligence community, the DHS, the Department of Justice, and other entities. The CNSS was formed in 2001 by Executive Order 13231; it evolved from the National Security Telecommunications and Information Systems Security Committee, which had been created in 1990. The executive agency for the CNSS is the National Security Agency (NSA).

The Federal Information Security Management Act of 2002 defines NSS as follows:

> *(2)(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—*
>
> > *(i) the function, operation, or use of which—*
> >
> > > *(I) involves intelligence activities;*
> > >
> > > *(II) involves cryptologic activities related to national security;*
> > >
> > > *(III) involves command and control of military forces;*
> > >
> > > *(IV) involves equipment that is an integral part of a weapon or weapons system; or*
> > >
> > > *(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or*
> >
> > *(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.*
>
> *(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).*[23]

Or, as the DoD explains, an NSS is—

> *A telecommunications or information system operated by the Federal Government that involves intelligence activities; cryptologic activities related to national security; command and control of military forces; equipment that is an integral part of a weapon or weapons system; or that is critical to the direct fulfillment of military or intelligence missions.*[24]

22 National Institute of Standards and Technology, *Announcing Approval of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems* (Gaithersburg, MD: Computer Security Division, March 2006), https://www.federalregister.gov/documents/2006/03/31/E6-4720/announcing-approval-of-federal-information-processing-standard-fips-200-minimum-security.

23 FISMA, Pub. L. No. 107-347, Title III (December 17, 2002).

24 Inspector General, Department of Defense, "DoD's Policies, Procedures, and Practices for Information Security Management of Covered Systems" (Report No. DODIG-2016-123, Department of Defense, Alexandria, VA, August 15, 2016), http://www.dodig.mil/pubs/documents/DODIG-2016-123.pdf.

Thus, NSS encompass more than military or intelligence systems, or various levels of classified information.[25] For example, the Department of Energy has NSS by virtue of its mission to maintain the nuclear weapons stockpile. Similarly, other agencies including the Departments of Energy, State, Treasury, and Justice all have roles in intelligence, a mission not limited to agencies such as the Central Intelligence Agency and the DoD.

Although the CNSS was established to develop operating policies, procedures, guidelines, instructions, and standards for NSS, FISMA specifically grants the Secretary of Defense and the Director of Central Intelligence separate, individual authority over their own systems. As stated in a 2002 House Committee on Government Reform report, "This guidance is not to govern such systems, but rather to ensure that agencies receive consistent guidance on the identification of systems that should be governed by national security system requirements."[26]

EXECUTIVE BRANCH AND SCRM

Congress is not alone in its ability to influence NIST and federal ICT policy; actions by the Executive Branch have advanced the ICT and SCRM agenda in important ways.

The Comprehensive National Cybersecurity Initiative was established by President George W. Bush in January 2008 through National Security Presidential Directive 54/Homeland Security Presidential Directive 23 and expired under President Barack Obama.[27] The directive established the foundation for current DoD policy on cybersecurity issues and provided the initial impetus to the DoD's SCRM efforts by including funding for pilot programs and reports on results, elements of which were the basis for subsequent comprehensive enterprise SCRM programs. The directive called for the Secretaries of Defense and Homeland Security, in coordination with the Secretaries of the Treasury, Energy, and Commerce; the Attorney General; the Director of National Intelligence; and the Administrator of General Services, to develop a strategy and implementation plan to, among other issues, "better manage and mitigate supply chain vulnerabilities," including specific recommendations for the federal government and defense acquisition process. The CNCI itself aimed to reduce federal ICT vulnerabilities and prevent intrusions; strengthen supply chain security; and enhance research, development, education, and investment in key technologies. The DHS and DoD were the lead agencies for the SCRM initiative, but the directive and its related activities remained classified. A March 2010 report on the initiative by the Government Accountability Office noted that the classification level hindered efforts by the Department of State and the National Cyber Security Center to engage outside organizations, including the private sector.[28]

In March 2010, the DoD issued DoD Directive-Type Memorandum 09-016–SCRM to Improve the Integrity of Components Used in DoD Systems. The directive defined SCRM and supply chain risk, and stated that supply chain risk shall be addressed early and across the entire system lifecycle through a defense-in-breadth approach to managing the risks to the integrity of ICT within covered systems.

25 Further details on the connection between NSS and classified information can be found in National Security Agency, *CNSSI No. 1253: Security Categorization and Control Selection for National Security Systems* (Ft. Meade, MD: CNSS Secretariat, March 2014), http://www.dss.mil/documents/CNSSI_No1253.pdf; and National Security Agency, *CNSSI No. 1253 Attachment 5: Classified Information Overlay* (Ft. Meade, MD: CNSS Secretariat, May 2014), http://cryptome.org/2014/05/cnss-classified-info-overlay.pdf.

26 National Institute of Standards and Technology, *NIST Special Publication 800-59: Guideline for Identifying an Information System as a National Security System* (Gaithersburg, MD: Computer Security Division, August 2003), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-59.pdf; U.S. House of Representatives, "Report of the Committee on Government Reform" (Report 107-787, November 14, 2002), 85, quoted in NIST Special Publication 800-59.

27 "National Security Presidential Directive/NSPD-54 and Homeland Security Presidential Directive/HSPD-23," The White House, (Washington, DC, January 8, 2008, https://www.georgewbushlibrary.smu.edu/~/media/GWBL/Files/Digitized%20Content/2014-0390-F/t030-021-012-nspd54-1-20140390f.ashx.

28 U.S. Government Accountability Office, "Cybersecurity: Progress Made by Challenges Remain in Devining and Coordinating the Comprehensive National Initiative" (GAO-10-338, Washington, DC, March 2010), http://www.gao.gov/new.items/d10338.pdf.

Directive-Type Memorandum 09-016 was subsumed in November 2012 by DoD Instruction 5200.44, which was modified by Change 1 in August 2016.[29] The 2012 Instruction considers National Security Presidential Directive 54/Homeland Security Presidential Directive 23 the basis for the directive's SCRM implementation strategy, along with the following references:

- National Security Presidential Directive 54/Homeland Security Presidential Directive 23, "Cybersecurity Policy," January 8, 2008
- Section 806 of Public Law 111-383, "The National Defense Authorization Act for Fiscal Year 2011," January 7, 2011
- DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
- DoD Instruction 5000.02, "Operation of the Defense Acquisition System," December 8, 2008 (updated January 7, 2015)
- DoD Instruction 8500.01, "Cybersecurity," March 14, 2014 (from DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002)
- Committee on National Security Systems Directive No. 505, "Supply Chain Risk Management (SCRM)," March 7, 2012[30]

Military and intelligence systems are a subset of NSS, rather than the other way around, and DoD SCRM policies have largely been developed by the DoD itself, or by the DoD in concert with other members of the CNSS.

In 2013, President Obama's Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," provided an influential but unanticipated boost to SCRM policy. The executive order focused on improving the cybersecurity of "Section 9 entities," or "critical infrastructure where a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security."[31] The order does not mention supply chain or SCRM, but it tasks NIST with creating "a framework to reduce cyber risks to critical infrastructure," including "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." This framework would become the NIST Cybersecurity Framework (NIST CSF).

The NIST CSF, published in February 2014, created the Identify, Protect, Detect, Respond, and Recover framework now ubiquitous throughout federal discussions of cybersecurity.[32] Supply chain issues make a brief appearance in the Business Environment category of the Identify section of the framework, which instructs organizations to identify their role in the supply chain. The framework highlights NIST SP 800-53 Rev. 4 as an informative reference for this subcategory. Other SCRM developments continued gradually from previous lines of effort, as when a revision to NIST SP 800-37, released in June 2014, briefly mentioned SCRM with respect to external providers of ICT products.[33] The NIST CSF now underpins much of the discussion surrounding federal ICT cybersecurity, and thus SCRM, for federal ICT networks. Despite the framework's origins as an effort focused on critical infrastructure, it has been adopted by numerous federal organizations.

29 Department of Defense, "Department of Defense Instruction 5200.44" (August 25, 2016), https://www.hsdl.org/?abstract&did=795012.

30 National Security Agency, *CNSSD No. 505: Supply Chain Risk Management* (Ft. Meade, MD: CNSS Secretariat, March 7, 2012), https://info.publicintelligence.net/CNSS-SupplyChainRisk.pdf.

31 The White House, "Executive Order—Improving Critical Infrastructure Cybersecurity" (Office of the Press Secretary, Washington, DC, February 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

32 National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (February 12, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

33 National Institute of Standards and Technology, *NIST Special Publication 800-37 Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Live Cycle Approach* (Gaithersburg, MD: Computer Security Division, February 2010), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf.

CONGRESSIONAL ACTION AND SCRM

The Federal Information Technology Acquisition Reform Act (FITARA), FISMA, and the Cybersecurity Enhancement Act currently delineate the bounds of debate surrounding federal ICT risk management.

Federal Information Technology Acquisition Reform Act

Although introduced in 2013, the final version of FITARA did not become law until late 2014, when it passed as part of the FY 2015 National Defense Authorization Act.[34] FITARA had seven primary focus areas:

1. Enhancing the authority of the chief information officer
2. Enhancing transparency and improved risk management in IT investments
3. Requiring savings through IT portfolio review
4. Expanding the training and use of IT cadres
5. Consolidating federal data centers
6. Maximizing the benefit of the Federal Strategic Sourcing Initiative
7. Expanding government-wide software purchasing programs

FITARA tasked the OMB with implementing a process for ICT portfolio review and reviewing ICT acquisition staffing demands. FITARA was passed with fiscal concerns in mind and is commonly understood as an attempt to properly plan and manage incredibly expensive IT acquisitions. Congress views FITARA primarily as a fiscal oversight initiative designed to prevent costly spending, rather than as a security policy. Conversations between Interos leadership and congressional offices revealed Congress is reluctant to securitize FITARA by adding SCRM elements to the policy, such as requiring baseline vendor vetting prior to approving acquisitions. However, like previous policy efforts, FITARA has affected supply chain issues indirectly.

FITARA helps federal chief information officers increase visibility over their ICT infrastructure, potentially reducing vulnerabilities due to lack of oversight and transparency of what systems exist and therefore need some aspect of security. Perhaps somewhat paradoxically, however, FITARA's focus on portfolio review encourages agencies to identify aging infrastructure elements and consolidate them through new technologies. Portfolio review encourages modernization, and modernization introduces new COTS products into federal ICT systems. Due to the nature of global ICT supply chains, most new products that will enter federal ICT systems will include components originating in China or produced by Chinese firms. The use of COTS presents some challenges, given the confidentiality, integrity, and accessibility requirements for federal systems. In September 2017, FedScoop announced the results of a survey of 200 federal IT executives conducted by Unisys Corporation and the research company Market Connections. Fifty-nine percent of survey respondents said IT modernization efforts have increased the cybersecurity challenges they face.[35]

A lack of compliance with FITARA can be an indicator of cybersecurity vulnerabilities resulting from aging and poorly maintained ICT infrastructure, including vulnerabilities originating from supply chain risks. More important, a chief information officer's limited oversight of their federal IT systems creates potential gaps in security. This said, compliance with FITARA does not itself directly equal achieving comprehensive cybersecurity or oversight of a federal ICT supply chain.

The Modernizing Government Technology Act could place similar pressure on federal agencies. The bill was introduced by U.S. Representative Will Hurd (R-TX), chairman of the House Information Technology Subcommittee, in September 2016.[36] The act creates a $500 million central modernization fund that agencies can

34 Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015, H.R. 3979, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/house-bill/3979.

35 Carten Cordell, "IT Modernization Efforts Increase Cybersecurity Challenges, Survey Says," FedScoop, September 6, 2017, https://www.fedscoop.com/survey-modernization-efforts-increasing-cybersecurity-challenges/.

36 Modernizing Government Technology Act of 2016, H.R. 6004, 114th Cong. (2015–2016), https://www.congress.gov/bill/114th-congress/house-bill/6004.

borrow against to update aging IT systems.[37] The act also creates working IT capital funds that allow agencies to retain savings achieved from ongoing modernization efforts, provided they are used for future modernization projects. The bill was amended to the Senate version of the National Defense Authorization Act, which was passed by Congress in November 2017 and signed into law on December 12, 2017.[38]

The Modernizing Government Technology Act seems to presume that legacy equipment and systems are the sole source of risk, and that this risk can be mitigated through modernization. But modernization will actually increase risk if newly adopted technologies are not assessed appropriately before being integrated into federal IT networks. The bill establishes responsibilities and financial rewards to the agencies for modernizing their IT infrastructure and names the OMB and GSA as permanent members of a supervisory board, but it does not require any measure of supply chain security as part of modernization efforts. In the memorandum on "Implementation of the Modernizing Government Technology Act" signed by OMB Director Mick Mulvaney on February 27, 2018, there are multiple pages of guidelines for the execution of the program, but no requirement for SCRM as part of an agency's request for modernizing funds.[39]

As federal agencies face additional pressure from efforts like FITARA and the Modernizing Government Technology Act, the need for robust ICT SCRM leadership as well as an appropriately resourced capability becomes ever more important, affecting the ICT products agencies acquire, how and at what speed they acquire them, the suppliers they use, and the eventual quality and security over the product lifecycle.[40]

Federal Information Security Modernization Act and Circular A-130

FISMA sought to centralize federal cybersecurity management with the DHS, retaining the OMB's authority over policies for federal information systems but charging the DHS with the implementation of those policies. The bill retained the prerogatives of the Secretary of Defense and the Director of National Intelligence for their own systems. Although FISMA 2014 required continuous cybersecurity monitoring, sparking the DHS-led Continuous Diagnostics and Mitigation program, FISMA did not address SCRM specifically, creating yet another gap in federal laws and regulations.

The passage of FISMA 2014 also tasked NIST with continuing its work to protect federal information systems. In April 2015, NIST released SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations," the most detailed NIST contribution to the SCRM discussion since the creation of Control SA-12 in 2010. NIST SP 800-161 adopted the definition of risk from FIPS 200 to establish a definition for ICT supply chain risk and built on NIST SP 800-53 Rev. 4 and NIST Interagency Report 7622, *National Supply Chain Risk Management Practices for Federal Information Systems*, to enhance the overlay of ICT-specific SCRM controls.[41]

The OMB incorporated the new FISMA requirements and NIST controls into active policy. In support of FISMA 2014, the OMB issued Circular A-123 and revised Circular A-130 in July 2016. Circular A-123 broadened the scope of risk management beyond fiscal compliance and required federal organizations to establish an enterprise risk management capability, of which A-130 and SCRM are key components.[42] The release of a revised Circular A-130

37 National Defense Authorization Act for Fiscal Year 2018, H.R. 2810, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/2810.

38 Jason Miller, "In the End, Senate Lets the MGT Act in the Defense Bill," *Federal News Radio*, September 19, 2017, https://federalnewsradio.com/legislation/2017/09/in-the-end-senate-lets-the-mgt-act-in-the-defense-bill/; Carten Cordell, "Trump Signs Modernizing Government Technology Act into Law," FedScoop, December 12, 2017, https://www.fedscoop.com/trump-signs-mgt-act-law/.

39 The White House, "M-18-12, OMB Memorandum, Implementation of the Modernizing Government Technology Act" (Washington, DC: Office of Management and Budget, February 27, 2018), https://www.whitehouse.gov/wp-content/uploads/2017/11/M-18-12.pdf

40 "The Importance of SCRM's Role in Connection to FITARA," Interos Solutions, February 9, 2015, https://interosblog.wordpress.com/2015/02/09/the-importance-of-scrms-role-in-connection-to-fitara/.

41 National Institute of Standards and Technology, *NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations* (Gaithersburg, MD: Computer Security Division, April 2015), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf.

42 KMPG International, "A-123 Aims to Strengthen Government with Enterprise Risk Management," Government Executive, January 5, 2017. http://www.govexec.com/govexec-sponsored/2017/01/-123-aims-strengthen-government-enterprise-risk-management/134386/; The White House, "M-16-17, OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control" (Washington, DC: Office of Management and Budget, July 15, 2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-17.pdf.

was key, as it had not been updated since 2000.[43] The circular expanded on risk management issues and included specific supply chain security language. Perhaps most important, the circular requires agencies to implement security policies issued by the OMB, including standards and guidelines contained in NIST products, and formally establishes a shift from three-year review and authorizations of compliance activities to continuous monitoring of those activities. Appendix I of the circular details general requirements, implementation of FITARA, and SCRM principles.[44] The circular requires agencies to develop SCRM plans as described in NIST SP 800-161 and to satisfy the information security requirements in FIPS 200 and the security control baselines in NIST SP 800-53. It should be noted that as of the writing of this report, there has been no known audit to ensure federal agencies have impactful SCRM programs in place, nor is there policy that mandates a government-wide national supply chain risk management strategy.

Cybersecurity Enhancement Act

As part of the implementation of President Obama's Executive Order 13636, Congress modified NIST's mission in the Cybersecurity Enhancement Act of 2014, to have NIST continue work on the CSF and expanded the use of the CSF to owners and operators of critical infrastructure.[45]

This call for owners and operators of critical infrastructure to take NIST's work into account appears to be part of a broader move toward consolidating parts of the federal ICT policy framework. DoD Instruction 8500.01, issued in March 2014, required the DoD to implement system security controls designed by NIST, but it is DoD Instruction 5200.44, Change 1, effective August 2016, that explicitly adds NIST SP 800-161 as a basis for the implementation of the DoD SCRM strategy. Similarly, the CNSS released a revision of CNSS Directive 505, "Supply Chain Risk Management," in August 2017, replacing the directive published in March 2012.[46] The new directive makes explicit connections between the CNSS and NIST, explaining that the CNSS adopts NIST standards where applicable and publishes additional guidelines in instances where NIST does not sufficiently address the needs of NSS.

A new revision of the CSF was released for comment in January 2017, providing new details on managing cyber supply chain risks, clarifying key terms, and introducing measurement methods for cybersecurity. It also includes references to SCRM across all five components of the framework.[47] Increasingly integrating SCRM into federal risk management efforts is important to successfully managing the ICT modernization efforts envisioned in legislation like FITARA, but there remains no centralized leadership for federal SCRM efforts. Additionally, existing regulations and requirements do not adequately address the risk posed by COTS products, or risks related to ICT products linked to China or other state actors that may pose a threat to the United States.

43 The White House, "M-16-17."

44 Jason Miller, "OMB Initiates Cyber Marathon with Long-Awaited Policy Update," *Federal News Radio*, October 21, 2015, https://federalnewsradio.com/omb/2015/10/omb-initiates-cyber-marathon-long-awaited-policy-update/.

45 Cybersecurity Enhancement Act of 2014, S. 1353, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/senate-bill/1353/text; "NIST Releases Update to Cybersecurity Framework," National Institute of Standards and Technology, January 10, 2017, https://www.nist.gov/news-events/news/2017/01/nist-releases-update-cybersecurity-framework.

46 National Security Agency, *CNSSD No. 505: Supply Chain Risk Management* (Ft. Meade, MD: CNSS Secretariat, July 26, 2012), https://1yxsm73j7aop3quc9y5ifaw3-wpengine.netdna-ssl.com/wp-content/uploads/2017/08/CNSSD_505_Final2-Published-08-01-2017.pdf.

47 "NIST Releases Update," National Institute of Standards and Technology.

Chapter 3: Supply Chain Analysis of Federal ICT Manufacturers

As previously stated, this study uses a comprehensive definition of "U.S. government ICT supply chains" that includes (1) primary suppliers, (2) tiers of suppliers that support prime suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. The reason for this, as outlined below, is that the greatest risks are often unknown and driven directly by the location of the multiple tiers of suppliers and the nature of their third-party affiliations.

SUPPLIER LOCATION

No laws or regulations mandate that federal IT suppliers provide multi-tier transparency regarding their supply chains; however, HP, Dell, and Microsoft have embraced industry transparency principles in a way that allows some insight into their first-tier suppliers. All three publish lists of their primary suppliers, a practice that is not standard across the industry.[48] The lists are not constructed identically, so the data require some manipulation before they can be analyzed. Dell provides site addresses for all of its tier-one suppliers; HP provides site addresses for its final assembly suppliers but not for its commodity and component suppliers; and Microsoft provides a list of the names of its top 100 suppliers.[49]

For this paper, Interos analyzed the publicly reported supplier networks of HP, Dell, and Microsoft. Of the 344 identified suppliers for HP, Dell, and Microsoft, it was possible to identify a site address for 212. The 132 suppliers for which a site address could not be identified were categorized according to the location of their corporate headquarters. As expected, HP, Dell, and Microsoft source from the same companies; at times from the same company at the same site. As an example, all three source from Pegatron Corporation. Dell identified two site addresses from which it does business with Pegatron—one in Taoyuan City, Taiwan, and one in Jiangsu, China. HP also reported sourcing from the Jiangsu site. Because Microsoft reported sourcing from Pegatron, but did not identify a site, Microsoft was categorized as sourcing from Pegatron's headquarters in Taipei, Taiwan. Thus, the combined supplier list includes three entries for Pegatron: one for Taoyuan City, Taiwan; one for Jiangsu, China; and one for the Taipei, Taiwan headquarters. Using this categorization system, the unified suppliers list identifies 39 percent of suppliers to these three companies as located in China, 15 percent located in Taiwan, 13 percent located in the United States, and 8 percent located in Japan.

The links to China are more numerous than these data suggest, because a number of companies were categorized only by the location of their company headquarters. For the 132 companies for which a site address could not be conclusively determined, 87 were headquartered in Taiwan, the United States, or Japan. The unified supplier list categorizes these 132 suppliers only by the location of their headquarters, not by any supplier sites that may be elsewhere, yet it is common for companies headquartered in Taiwan, the United States, Japan, and other countries to base their production facilities in China. It is likely that a significant portion of these companies have operations in China, making China's influence on these supply chains larger than it appears at first glance.

SUPPLIER FINANCING AND INFLUENCE

Financial links to suspect entities, including state-owned or substantially state-controlled enterprises, are also important for SCRM, as they indicate potential vectors for nefarious influence. Previous reports have raised concerns about the connections between Intel, HP, Dell, IBM, Cisco, Microsoft, and Chinese entities such as

48 Apple follows similar transparency policies. Apple is a not a top 10 provider of enterprise ICT to the U.S. federal government, however, so its data were not included in this analysis.

49 Nick Wingfield and Charles Duhigg, "Apple Lists Its Suppliers for 1st Time," The New York Times, January 13, 2012, http://www.nytimes.com/2012/01/14/technology/apple-releases-list-of-its-suppliers-for-the-first-time.html; "HP Suppliers," Hewlett-Packard, http://h20195.www2.hp.com/V2/GetPDF.aspx/c03728062.pdf; "Our Suppliers," Dell, About Dell, Corporate Social Responsibility, Supply Chain, http://www.dell.com/learn/us/en/uscorp1/cr-social-responsibility; "Microsoft Top 100 Production Suppliers," Microsoft, http://download.microsoft.com/download/0/1/4/014D812D-B2E3-43A0-A89A-16E3C7CD46EE/Microsoft_Top_100_Production_Suppliers_2016.pdf.

Tsinghua Holdings, Inspur Group, Beijing Teamsun Technology, and the China Electronics Technology Group Corporation (CETC).[50] In the analysis of suppliers for HP, Dell, and Microsoft, 28 suppliers (that accounted for 52 supplier site locations) were identified as presenting some level of risk owing to their connections to Chinese state-owned entities. **Table 2** includes information on several of these entities of concern. Risk can be present in the nature of the government's relationship with an entity: "state-controlled" entities listed below function in some ways as part of official government or military institutions; "state-owned" entities have significant financial ownership or control by the state; "state-influenced" entities may have other, less formal, ties to a government, such as strategic partnerships or leadership connections; and "defense suppliers" provide services or products to a state's government, military, or security services.

For this report, Interos complied a listing of entities, their potential risk based on the relation to the Chinese government, and the publicly available sources this information was garnered from. Further research would need to be completed to truly understand the comprehensive risk these entities may pose to U.S. ICT supply chains.

Table 2
Examples of Federal ICT Suppliers Connected to Entities of Concern

Entity Name	Risk	Details	Source
Beijing Teamsun Technology	Defense supplier	Partnership with IBM.	Various.
BOE Global	State-owned	Supplies display/liquid crystal display to Dell.	15.24 percent owned by Beijing State-Owned Assets Supervision and Administration.
China Electronics Technology Group Corporation (CETC)	State-controlled Defense supplier	A network of former military labs that operates both commercial and military technology businesses. Strategic partnerships with Microsoft and IBM.	State-owned company according to Dow Jones.
Chinese Academy of Sciences (CAS)	State-controlled	Connections to Chinese military, nuclear, and cyberespionage programs. Often appears as an investor or partner of other Dell, HP, or Microsoft suppliers.	Various.
Huawei	National champion	Cyberespionage risk.	U.S. House Permanent Select Committee on Intelligence Investigative Report.
Inspur Group	Defense supplier	Joint ventures and partnerships with Cisco, Intel, and IBM.	Various.
Legend Capital/ Holdings	State-controlled	Asset management arm of the CAS, and the owner of Lenovo. Occasionally appears as an investor or partner of other Dell, HP, or Microsoft suppliers. Part of a consortium that acquired Lexmark in 2016.	Various.
Lenovo	State-owned	Cyberespionage risk.	29.10 percent owned by Legend Holdings Corp.
Lexmark	State-influenced	Acquired in April 2016 by a consortium including Legend Capital. History of security vulnerabilities. Supplies accessories/printers to Dell.	Various.
Lishen Power Battery Systems Co. Ltd.	State-owned	CETC is sole shareholder. Supplies batteries to Dell.	State-owned company according to Dow Jones.
Tianma Microelectronics (USA) Inc. .	State-owned	Owned by China defense supplier. Supplies displays to Microsoft	20.81 percent owned by AVIC International Holdings Ltd. and 11.35 percent owned by the State-Owned Assets Supervision and Administration Commission.

50 "U.S. Tech Companies and Their Chinese Partners with Military Ties," *The New York Times*, October 30, 2015, https://www.nytimes.com/interactive/2015/10/30/technology/US-Tech-Firms-and-Their-Chinese-Partnerships.html.

Entity Name	Risk	Details	Source
TPV Technology Ltd.	State-owned	Supplies display/liquid crystal display to Dell and HP.	37.05 percent owned by the State-Owned Assets Supervision and Administration Commission.
Tsinghua Holdings	State-controlled	Asset management group focused on technology and defense sector. Joint ventures and strategic partnerships with Intel, HP, Dell, and IBM.	State-owned company according to Dow Jones.
Shenzhen Laibao Hi-Tech Co. Ltd	State-owned	Supplies display/liquid crystal display to Dell and HP.	20.91 percent owned by the State-Owned Assets Supervision and Administration Commission.
Zhongxing Telecommunications Corporation	National champion	Cyberespionage risk.	U.S. House Permanent Select Committee on Intelligence Investigative Report.

Source: Interos Solutions.

Entities that present the most risk to the supply chain are those that exhibit close ties to Chinese government entities, particularly entities involved in China's military, nuclear, or cyberespionage programs. For example:

- Dell supplier Lishen Power Battery Systems Co. Ltd. is a subsidiary of Tianjin Lishen Battery Joint-Stock Company Limited, an SOE affiliated with CETC, which is a network of former military labs that operates both commercial and military technology businesses. CETC appears to be Lishen's sole shareholder.[51]

- Hengdian Group DMEGC Magnetics Co. Ltd. supplies magnetic materials to Microsoft, and is a subsidiary of Hengdian Group Holdings. The group's website states it is an enterprise approved by the Chinese Academy of Sciences (CAS) and China's Ministry of Science and Technology, and has cooperated with the state-owned China National Nuclear Corporation.[52]

- GoerTek Inc. supplies acoustic components to Microsoft. In addition to state-backed investment from China International Fund Management Co., Ltd., the company has long-term strategic partnerships with the CAS and universities linked to China's cyberespionage programs, such as Tsinghua University, Zhejiang University, and Harbin Institute of Technology.[53] Other customers include Lenovo.[54]

The connections between these firms and entities involved in China's military, nuclear, or cyberespionage programs increase risk associated with federal ICT providers sourcing products or services from these firms. This risk could present itself as a supply chain attack through a compromised product, such as batteries or acoustic components supplied to federal ICT providers. Still other Chinese SOEs supply federal ICT providers with magnets, shielding materials, or cables and power connectors.[55] These products could present risk if they are of inferior quality and fail to operate, but they are unlikely to present significant cybersecurity risk to federal ICT networks. The risk might also stem from more subtle actions, including by federal ICT providers revealing design information, product specifications, or other sensitive information to their suppliers as part of standard business practices. Business information that may be innocuous when passed to a standard business partner becomes less innocuous when passed to individuals or entities associated with a rival government.

A good SCRM program assesses the risks associated with the nature of a particular product in tandem with the risks stemming from the entity that is producing or providing the product. Assessing the supply chain risks associated with liquid crystal displays (LCDs) is one example of this process. Displays are not as critical to an end-product

51 "Shareholder's Info," Lishen, About Lishen, accessed October 29, 2017, http://en.lishen.com.cn/textContent.aspx?cateid=181&bigcateid=171.
52 "History," Hengdian Group, About Us, accessed March 23, 2018, from Internet Archive WayBackMachine, https://web.archive.org/web/20170415230303/http://www.hengdian.com/site/en/en_com_history.htm.
53 "Partners," Goertek, About Us, accessed March 23, 2018, http://www.goertek.com/en/about/hzhb.html.
54 "Goertek Announces Next-Gen VR Reference Design Powered by Snapdragon™ 845," PRNewswire, March 2, 2018, https://www.prnewswire.com/news-releases/goertek-announces-next-gen-vr-reference-design-powered-by-snapdragon-845-300607312.html.
55 "HP Suppliers," Hewlett-Packard; "Our Suppliers," Dell; "Microsoft Top 100 Production Suppliers," Microsoft.

as its microprocessor, but their hardware, firmware, and connections to other ICT products can make them an important component in an ICT supply chain. In 2016, security researchers from Red Balloon Security identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of their monitor displays.[56]

Several Chinese companies manufacture the LCDs that are a component of tablets, notebooks, and other computers produced by Microsoft, Dell, HP, and other federal ICT providers, and several of these companies have ties to the Chinese government or military. For example:

- Tianma Microelectronics supplies LCDs to Microsoft. The company's primary shareholders include AVIC International Holdings Ltd., the State-Owned Assets Supervision and Administration Commission (which manages the central government's SOEs), and the City of Wuhan. AVIC is an SOE that was formed in 2008 after the consolidation of China Aviation Industry Corporation I (AVIC I) and China Aviation Industry Corporation II (AVIC II).[57] AVIC is also one of China's largest defense suppliers, and makes aircraft for civilian and military uses, including bombers and fighter jets.

- Dell and HP both source LCDs from the state-owned TPV Technology Ltd. and Shenzhen Laibao Hi-Tech Co. Ltd. TPV Technology Ltd. is a China-based company that also does business as Top Victory Electronics Company and TPV-INVENTA Technology Co., Ltd. The company is controlled by state asset groups such as the State-Owned Assets Supervision and Administration Commission and China Greatwall Technology Group Co., Ltd. The State-Owned Assets Supervision and Administration Commission also controls 20 percent of Shenzhen Laibao Hi-Tech Co. Ltd. Dell also sources LCDs from six sites controlled by BOE Global, a company whose largest shareholder is the Beijing state-owned Capital Management Center.[58]

SUPPLY CHAIN RISK CASE STUDY: CORPORATE INTELLIGENCE-SHARING AGREEMENTS

An analysis of the business relationships of several top federal government ICT providers reveals corporate alliances and partnerships with SOEs in China as well as government-connected firms in Israel and Russia. Business relationships can affect multiple tiers within a single supply chain. While such networks of corporate alliance and partnership are common in the commercial sphere, they present security risks to federal ICT systems by potentially allowing nefarious actors access to technical information that could be used to infiltrate federal ICT systems. The information sharing inherent in commercial alliances can enable more efficient product integration and development. Commercial partnerships that share program application data, configuration information, or even deployment policies, however, may inadvertently grant malicious actors information they need to infiltrate federal ICT systems. Without a comprehensive SCRM program to investigate these partnerships, the connections and relationships may never be known, and the risk may remain undiscovered.

Intel and IBM: (In)Security Partnerships

Concerns associated with component production and manufacturing in China represent one facet of the supply chain risk facing the federal government's ICT system. As Chinese companies move up the value chain, the prospect of China-supplied software becomes ever more important to risk analysis. While an analysis of source code is generally not possible from unclassified sources, supply chain risks can be assessed on the basis of published business partnership announcements, including the establishment of corporate alliances.

Intel's Security Innovation Alliance allows partner companies to exchange threat intelligence and develop technology integrations with the McAfee Data Exchange Layer. The alliance produces integrated security solutions, by allowing technology partners to connect their products in a more efficient manner. The alliance includes companies (such as Huawei) with connections to the governments and security organizations of countries on

56 Lorenzo Franceschi-Bicchierai, "Hackers Could Break into Your Monitor to Spy on You and Manipulate Your Pixels," *Motherboard*, August 6, 2016, https://motherboard.vice.com/en_us/article/jpgdzb/hackers-could-break-into-your-monitor-to-spy-on-you-and-manipulate-your-pixels.

57 "Overview," AVIC, About Us, accessed October 29, 2017, http://www.avic.com/en/aboutus/overview/index.shtml.

58 Lexis Nexis, Dun and Bradstreet, Dow Jones, Hoovers Data Repository. Factiva Database, Dow Jones and Reuters, New York.

the intelligence community's sensitive countries list.[59] As part of the alliance, Huawei provides a Cybersecurity Intelligence System that collects network traffic information in order to detect attacks and provide investigation and evidence collection capabilities. Huawei Cybersecurity Intelligence System works with McAfee ePolicy Orchestrator and McAfee Active Response. Partner products are subject to engineering testing prior to integration, but the risk in these partnerships stems from the possibility that information, source code, or other details shared as part of the product integration process could also be used to identify and exploit vulnerabilities in a product.

In a 2012 report, Gartner noted that the technical challenges of technology integration and corporate collaboration present increasing risk to ICT supply chains: "Enterprises are opening up their internal IT networks and systems to collaborate and share information with customers, partners and suppliers. As a result, all of these become targets for IT supply chain compromise."[60] Intel is not alone in participating in these sorts of alliances. In 2000, IBM announced a collaborative agreement with Huawei, including an R&D effort.[61]

VMware Partnerships with Chinese SOEs and Kaspersky

VMware, a subsidiary of Dell, has entered into corporate partnerships with Chinese SOEs that could present national security vulnerabilities to U.S. federal ICT systems. VMware provides cloud computing and software virtualization services to the U.S. government and the private sector. Following Dell's acquisition of VMware's parent company, EMC, in September 2016, Dell controls approximately 82.8 percent of VMware's outstanding common stock.[62]

In April 2016, VMware set up its first China joint venture with Sugon, a Tianjin-based company that specializes in high-performance computers, servers, storage products, and software systems. Sugon's full English name is Dawning Information Industry. It was founded as Dawning Yunjisuan Technology Co. Ltd. in 1996 with backing from the CAS. Currently the Chinese government is the largest shareholder of Sugon, with the CAS retaining a 23 percent stake.[63] The VMware-Sugon joint venture is called VMsoft and provides cloud computing and virtualization software and services. VMware holds a 49 percent stake in VMsoft, while Sugon holds a 51 percent stake.[64]

VMware also has product relationships with Kaspersky Lab,[65] the Russia-based cybersecurity and antivirus software company recently named in the DHS's divestment directive.[66] Kaspersky is a Russian-owned cybersecurity provider whose founder and CEO used to work for the KGB, the security service of the former Soviet Union.[67] A recent reported shift in the leadership of Kaspersky Labs has seen people with close ties to Russian military and intelligence services filling more executive positions. Speculation exists that these executives actually participate

59 Warwick Ashford, "Check Point, Huawei Join Intel Security Innovation Alliance," *Computer Weekly*, November 3, 2016, http://www.computerweekly.com/news/450402310/Check-Point-Huawei-join-Intel-Security-Innovation-Alliance; "Huawei Joins Intel Security Innovation Alliance to Defend Customers against Security Threats," Huawei, News, November 4, 2016, http://www.huawei.com/en/news/2016/11/Huawei-Joins-Intel-Security-Innovation-Alliance; "McAfee Security Innovation Alliance Partner Directory," McAfee, Business Home, Partners, McAfee Security Innovation Alliance, accessed October 29, 2017, https://www.mcafee.com/us/partners/partnerlisting.aspx.

60 "Maverick*Research: Living in a World without Trust: When IT's Supply Chain Integrity and Online Infrastructure Get Pwned," Gartner, October 5, 2012, http://www.energycollection.us/Energy-Security/Living-World-Without-Trust-Filed.pdf.

61 IBM, "IBM and Huawei Announce Networking Technology Collaboration," news release, September 25, 2000, https://www-03.ibm.com/press/us/en/pressrelease/1541.wss.

62 VMware, Inc., "10-K Annual Report 2016," retrieved October 25, 2017, from SEC EDGAR database, https://www.sec.gov/Archives/edgar/data/1124610/000112461017000009/vmw-1231201610xk.htm.

63 Tom Wilkie, "Chinese Government Kicks Commercial Companies Overseas," *Scientific Computing World*, August 25, 2015, https://www.scientific-computing.com/feature/chinese-government-kicks-commercial-companies-overseas.

64 Jane Ho, "VMware Sets up First China Joint Venture with High-Performance Computer Maker Sugon," *Forbes*, May 24, 2016, https://www.forbes.com/sites/janeho/2016/05/24/VMware-sets-up-first-china-joint-venture-with-high-performance-computer-maker-sugon/#257d64db20af.

65 "Kaspersky Agentless Virtualization Security," Kaspersky, Products, accessed October 30, 2017, https://usa.kaspersky.com/small-to-medium-business-security/virtualization-agentless; Department of Homeland Security, "DHS Statement on the Issuance of Binding Operational Directive 17-01," press release, September 13, 2017, https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01; "Kaspersky Security for Virtualization 3.0 Agentless Service Pack 1 (2134021)," VMware, last updated October 16, 2015, https://kb.vmware.com/s/article/2134021.

66 On September 13, 2017, the DHS issued a directive ordering federal departments and agencies to identify, discontinue to use, and ultimately remove the Kaspersky products from federal information systems. This directive was issued amid concerns that the Russian government and Russian intelligence agencies may use Kaspersky products to compromise federal information systems.

67 Pamela Engel, "Why One of the World's Leading Cyber-espionage Firms Won't Touch Russia," *Business Insider*, March 19, 2015, http://www.businessinsider.com/kaspersky-and-russian-spies-2015-3.

in investigations on behalf of the Russian government and may share Kaspersky customers' data with the government.[68] Reports by *BloombergBusinessweek* from July 2017 cited internal Kaspersky emails alleging that Kaspersky personnel have accompanied Russian intelligence and police on raids and arrests.[69] A report from *The Wall Street Journal* in October 2017 shed additional light on an incident in 2015, in which hackers working for the Russian government used Kaspersky's antivirus software running on an NSA contractor's personal computer to steal details about how the United States penetrates foreign computer networks and defends against cyberattacks.[70] The U.S. government has been progressively blocking agencies from using Kaspersky. The National Defense Authorization Act for Fiscal Year 2018, signed into law in December 2017, included a ban on using "hardware, software, or services developed or provided, in whole or in part" by Kaspersky Lab, its successors, or affiliated entities.[71]

These types of business relationships can introduce risk through multiple relationships at different tiers within a single supply chain. Kaspersky's products integrate with virtual machine platforms such as Microsoft Hyper-V, Citrix XenServer, and Kernel-based Virtual Machine.[72] Kaspersky is a "VMware Integrated Partner Solutions for Networking and Security" provider, as well as one of the six partners VMware recommends for antivirus and protection solutions.[73] VMware also has a relationship with vArmour Networks, Inc., a virtual data center and cloud security company,[74] and vArmour has a partnership with Nutanix, which is itself a technology partner of Kaspersky.[75] Kaspersky antivirus products are integrated into routers, chips, and software products produced by Cisco, Juniper, D-Link, Broadcom, Amazon, and Microsoft.[76]

68 Carol Matlack, Michael Riley, and Jordan Robertson, "The Company Securing Your Internet Has Close Ties to Russian Spies," *BloombergBusinessweek*, March 20, 2015, https://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies.

69 Jordan Robertson and Michael Riley, "Kaspersky Lab Has Been Working with Russian Intelligence," *BloombergBusinessweek*, July 11, 2017, https://www.bloomberg.com/news/articles/2017-07-11/kaspersky-lab-has-been-working-with-russian-intelligence.

70 Gordon Lubold and Shane Harris, "Russian Hackers Stole NSA Data on U.S. Cyber Defense," *The Wall Street Journal*, October 5, 2017, https://www.wsj.com/articles/russian-hackers-stole-nsa-data-on-u-s-cyber-defense-1507222108.

71 National Defense Authorization Act for Fiscal Year 2018.

72 "Kaspersky Security for Virtualization," Kaspersky Lab, accessed October 30, 2017, http://media.kaspersky.com/en/business-security/Kaspersky%20Security%20for%20Virtualization%20Datasheet.pdf.

73 "VMware Integrated Partner Solutions for Networking and Security," VMware, accessed October 30, 2017, https://www.VMware.com/content/dam/digitalmarketing/VMware/en/pdf/products/vcns/VMware-integrated-partner-solutions-networking-security.pdf; "Antivirus Best Practices for VMware Horizon View 5.x," VMware, accessed October 30, 2017, https://www.VMware.com/content/dam/digitalmarketing/VMware/en/pdf/techpaper/VMware-View-AntiVirusPractices-TN-EN.pdf.

74 vArmour, "vArmour Distributed Security System Achieves VMware's Highest Level of Product Endorsement–VMware Ready," press release, September 16, 2015. https://www.varmour.com/past-press/94-varmour-distributed-security-system-achieves-VMware-s-highest-level-of-product-endorsement-VMware-ready.

75 Keith Stewart, "It's Official: vArmour and Nutanix Team up to Deliver Simple, Secure Data Centers," vArmour blog, July 8, 2015, https://www.varmour.com/resources/blog/entry/its-official-varmour-and-nutanix-team-up-to-deliver-simple-secure-data-centers; "vArmour," Nutanix, Technology Alliances, accessed October 30, 2017, https://www.nutanix.com/partners/technology-alliance-program/varmour/; "vArmour and Nutanix Partner to Simplify and Secure Hyper-Converged, Distributed Infrastructure," *Martekwired*, July 8, 2015, https://finance.yahoo.com/news/varmour-nutanix-partner-simplify-secure-120000717.html; "Recognition," Kaspersky, Solutions, Enterprise Security, Cloud Security, accessed October 30, 2017, https://usa.kaspersky.com/enterprise-security/virtualization.

76 Adam Mazmanian, "Kaspersky Axed from Governmentwide Contracts," *FCW*, July 12, 2017, https://fcw.com/articles/2017/07/12/kaspersky-gsa-nasa-intel.aspx.

Chapter 4: China's Political and Economic Agenda Is Behind the Supply Chain Security Dilemma

Understanding that Chinese national political and economic policies encourage indigenous ICT manufacturing and development helps explain the risks to the U.S. ICT supply chain. The PRC government justifies these policies in terms of ensuring China's own national security, but China's policies related to prioritizing indigenous production, extracting concessions from multinationals, using Chinese companies as state tools, and targeting U.S. federal networks and the networks of federal contractors have heightened risks to the U.S. ICT supply chain.

PRIORITIZING INDIGENOUS ICT PRODUCTION

The Chinese government has expended significant political and economic capital in its effort to expand and indigenize its ICT production capabilities. In the 1980s, China began to rival Japan and South Korea as a producer of low-tech IT components. China's production capacity expanded throughout the 1990s, and it began to move up the value chain, producing ever more complex electronic equipment. By the late 1990s, the Chinese domestic market itself became a factor in the evolving equation. The rising incomes of China's new middle class meant that the country was now an important consumer market for the very products it had once been known for producing and exporting. Multinational tech companies shifted production and supply centers to China, launched Chinese subsidiaries, and invested in Chinese manufacturing and R&D centers to meet demand from China's rapidly growing domestic market. These deals occurred in tandem with PRC outreach to foreign multinationals, as the country encouraged foreign investment that could bring new products, technologies, and, most important, jobs to China. **Table 3** is an overview of key PRC policies enacted during this period.

Table 3
Foundational PRC Policies for Indigenous ICT Development

Date	Title	Description
1986	National High Technology Research and Development Program (863 Program)	The 863 Program funds high-technology development in strategic sectors, including IT, biology, aeronautics, automation, energy, materials, and oceanography. Government institutes, university research labs, and SOE R&D departments participate in 863 initiatives. The Chinese Academy of Sciences is the largest recipient of 863 money. In 2014, the program provided more than $5 billion for China's microchip industry, developing software to compete with Microsoft's Windows and Google Inc.'s Android, and advancing China's server manufacturing capacity. Inspur Chairman Sun Pishu is a member of China's legislature and a member of the 863 Program's expert committee. In 2014, he proposed measures to review critical technology purchases and accelerate domestic innovation efforts.
2006	National Medium- and Long-Term Plan for Science and Technology Development Plan (2006–2020)	The goal is for China to be a major center of indigenous innovation by 2020 and a global innovation leader by 2050. This plan: • Seeks to sharply reduce the country's dependence on foreign technology • Increases gross expenditures for R&D, especially for space programs, aerospace development and manufacturing, renewable energy, computer science, and life sciences • Calls for regulations in the country's government procurement law to "encourage and protect indigenous innovation," requiring a first-buy policy for major domestically made high-tech equipment and products that possess proprietary intellectual property rights, providing policy support to enterprises in procuring domestic high-tech equipment, and developing "relevant technology standards" through government procurement

Source: James McGregor, Dow Jones.[77]

77 James McGregor, *China's Drive for "Indigenous Innovation": A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, Global Regulatory Cooperation Project, 2010), https://www.uschamber.com/sites/default/files/documents/files/100728chinareport_0_0.pdf; Dow Jones, "NSA Concerns Give Chinese Server Maker Inspur a Boost," *The Australian*, July 30, 2014, http://www.theaustralian.com.au/business/latest/nsa-concerns-give-chinese-server-maker-inspur-a-boost/news-story/b80feaa88eb98909ad47ea1bc11ae948.

In February 2017, the PRC State Council published a press release highlighting a recent IHS Markit report indicating China has moved from being a low-cost supplier to being the center of the global supply chain.[78] As Chinese firms move up the value chain, the Chinese government has shifted the focus of its development policies. Where once the PRC government offered tax incentives and other perks to encourage foreign direct investment (FDI), the Chinese domestic market now represents a significant draw. China is less likely to offer incentives to foreign companies to do business in China and more likely to demand concessions from them in exchange for the privilege, thereby creating even more opportunities for risk insertion into the global COTS ICT supply chain.

RAISING SECURITY CONCERNS

Since 2013, the Chinese government has put pressure on U.S. ICT companies to surrender source code, store data on servers based in China, invest in Chinese companies, and permit the PRC government to conduct security audits on ICT products. In the wake of Edward Snowden's 2013 allegations that the U.S. government used some of the country's technology firms to spy on foreign governments, Chinese officials began investigating Microsoft, Apple, and other U.S. technology companies.[79] Official media called for a "de-Cisco campaign" or a boycott of Cisco products.[80] In June 2013, the Chinese state-backed *China Economic Weekly* ran a cover story calling eight U.S. companies (Apple, Cisco, Google, IBM, Intel, Microsoft, Oracle, and Qualcomm) "guardian warriors" that had "seamlessly penetrated" Chinese society.[81]

Several elements of subliminal messaging are at work here. In a move directed primarily at U.S. observers and China's educated and globalized elite, the cover of the issue that contained this article reused a U.S. World War II poster originally released to warn against German espionage.[82] **Exhibit 3** compares the two images. The image on the left is a copy of the original poster released by the U.S. Office of Emergency Management in 1942. The image on the right is the cover of *China Economic Weekly* published in June 2013, modified by the addition of the NSA insignia on the soldier's helmet.

Exhibit 3
U.S. Espionage Drives China's Nationalist IT Policy

Sources: U.S. Office of Emergency Management (1942) and *China Economic Weekly* (2013).

78 "China Becomes Center of Global Supply Chain," State Council of the People's Republic of China, February 10, 2017, http://english.gov.cn/news/top_news/2017/02/10/content_281475564088064.htm.
79 Eva Dou, "NSA Concerns Give Chinese Server Maker a Boost," *The Wall Street Journal*, July 29, 2014, https://www.wsj.com/articles/nsa-concerns-give-chinese-server-maker-inspur-a-boost-1406653858.
80 Daniel H. Rosen and Beibei Bao, "Eight Guardian Warriors: PRISM and Its Implications for US Businesses in China," Rhodium Group, July 18, 2013, http://rhg.com/notes/eight-guardian-warriors-prism-and-its-implications-for-us-businesses-in-china-2.
81 Bai Zhaoyang 白朝阳, "Meiguo 'Bada Jingang' Shentou Zhongguo Da Qi Di" 美国"八大金刚"渗透中国大起底 [United States' "Eight Guardian Warriors" Seamlessly Penetrate China], *China Economic Weekly* 中国经济周刊, June 24, 2013, http://paper.people.com.cn/zgjjzk/html/2013-06/24/content_1259857.htm.
82 United States Office of Emergency Management, "He's Watching You" (1942), accessed from New Hampshire State Library, Unifying a Nation, https://www.nh.gov/nhsl/ww2/ww57.html.

More relevant to China's domestic audience, the labeling of the eight U.S. tech firms as "guardian warriors" recalls the Eight-Nation Alliance that intervened militarily in China between 1899 and 1901 to suppress the Boxer Rebellion. Views on the rebellion are diverse, but in general the episode marked the flagging legitimacy of the Qing dynasty and the growing strength of anti-foreign, anti-colonialist forces in Chinese politics. Current PRC rhetoric frequently couches the Boxer Rebellion in anti-imperialist, patriotic-nationalist terms, and the Eight-Nation Alliance as a group that facilitated the collapse of the last Chinese dynasty and foreign oppression. The eight guardian warriors, then, represent not only a pernicious threat to China's unity and independence but also a call for increased self-reliance in order to resist foreign influence. The *China Economic Weekly* article argues that while President Barack Obama made it illegal for U.S. agencies to purchase Chinese IT equipment without a federal cybersecurity investigation, no law requiring the investigation of U.S. companies yet existed in China.

In 2014, more allegations about NSA espionage efforts directed at China were reported by the German weekly *Der Spiegel* and the *New York Times*.[83] The reports alleged that in early 2009 the NSA began targeting Huawei, as well as Chinese ministries, banks, and then-president Hu Jintao. The Chinese government began to move against U.S. ICT companies soon after, launching antitrust investigations of Qualcomm and Microsoft, issuing a ban on Windows 8 on government computers, and raising concerns about the Apple iPhone's security. In response to this pressure, Apple has promised to build an R&D center in China.[84]

EXTRACTING CONCESSIONS FROM MULTINATIONALS

The FDI Regulatory Restrictiveness Index of the Organisation for Economic Co-operation and Development (OECD) measures statutory restrictions on FDI in 62 countries, including all OECD and G20 countries, and covers 22 sectors.[85] The index gauges the restrictiveness of a country's FDI rules by looking at the four main types of restrictions: (1) foreign equity limitations, (2) screening or approval mechanisms, (3) restrictions on the employment of foreigners as key personnel, and (4) operational restrictions such as restrictions on branching, capital repatriation, or land ownership. According to OECD data, China is the most restrictive of the G20 countries.[86]

In 2014 and 2015, the Chinese government ramped up implementation of laws and policies that raise market access concerns among ICT manufacturers and suppliers in the United States by threatening to decrease competition, favor Chinese firms over foreign firms, or extract concessions from multinational firms seeking to do business in China. Many of these laws and policies are discussed in depth in publications by the U.S. Chamber of Commerce, the Congressional Research Service, and the U.S.-China Economic and Security Review Commission.[87] **Table 4** offers a brief overview.

83 "NSA Spied on Chinese Government and Networking Firm," *Der Spiegel*, March 22, 2014, http://www.spiegel.de/international/world/nsa-spied-on-chinese-government-and-networking-firm-huawei-a-960199.html; David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times*, March 22, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

84 David Barboza, "How China Built 'iPhone City' with Billions in Perks for Apple's Partner," *The New York Times*, December 29, 2016, https://www.nytimes.com/2016/12/29/technology/apple-iphone-china-foxconn.html.

85 "FDI Regulatory Restrictiveness Index," Organisation for Economic Co-operation and Development, March 27, 2017, http://www.oecd.org/investment/fdiindex.htm.

86 The Group of Twenty (G20) is an international forum dedicated to international cooperation on financial and economic issues. Members of the G20 include many of the world's wealthiest nations, and collectively account for more than four-fifths of the world's gross domestic product, three-quarters of global trade, and almost two-thirds of the world's population.

87 James McGregor, *China's Drive for "Indigenous Innovation"*; Wayne M. Morrison, "China-U.S. Trade Issues," Congressional Research Service, February 9, 2017, 35; OECD, OECD Science, Technology and Innovation Outlook 2016; Nargiza Salidjanova et al., "Economics and Trade Bulletin," U.S.-China Economic and Security Review Commission, August 7, 2017, https://www.uscc.gov/sites/default/files/Research/August%202017%20Trade%20Bulletin.pdf; "Economics and Trade Bulletin," U.S.-China Economic and Security Review Commission, June 2, 2017, https://www.uscc.gov/sites/default/files/trade_bulletins/June%202017%20Trade%20Bulletin.pdf.

Table 4
Chinese Laws and Policies Related to ICT and National Security

Date Issued	Title	Description
May 2015	Notice of the State Council on Issuing "Made in China 2025"	Lays out a comprehensive plan to upgrade the Chinese manufacturing sector through the use of intelligent ICT (smart manufacturing). Sets nine priority tasks over 10 sectors, with five definitive projects, including new IT, robotics, aerospace, ocean engineering, and high-end rail transportation. Calls for strengthened security reviews for investment, mergers and acquisitions, and procurement in manufacturing sectors that are related to national economy and national security.
July 2015	National Security Law	Promotes domestic and indigenous innovation in key sectors. Enables the government to conduct "national security reviews" of "foreign commercial investment, special items and technologies, Internet information technology products and services, projects involving national security matters, as well as other major matters and activities, that impact or might impact national security."
July 2015	Guiding Opinions of the State Council on Actively Advancing "Internet+" Action	Aims to drive economic growth in China through the integration of internet technologies with manufacturing and business. Prioritizes upgrading and strengthening the security of the internet infrastructure, expanding access to the internet and related technologies, making social services more convenient and effective, and increasing both the quality and effectiveness of economic development.
January 2016	Counter-Terrorism Law	Requires telecommunications operators and internet service providers to provide technical interfaces, decryption, and other technical support assistance to public and state security organizations that are conducting activities to prevent or investigate terrorism.
July 2016	13th Five-Year Plan for Science and Technology Innovation	Aims to strengthen China's science and technology competitiveness and international influence and develop breakthroughs in core and critical technology areas in order to support economic restructuring and industrial upgrading.
November 2016	Cybersecurity Law	Restricts select data transfers out of China. Requires firms that fall under the critical information infrastructure to store their data inside China. Firms have until 2018 to comply with some data storage requirements. Requires firms that interact with the critical information infrastructure or that provide services that may affect national security to be subject to a security review by Chinese authorities. This review may be used to ensure that these services are "secure and controllable," a term used in other Chinese digital regulations, which compels foreign firms to hand over important intellectual property assets such as source code to Chinese authorities for inspection.
November 2017	Standardization Law of People's Republic of China	Revises China's 1989 Standardization Law in ways that may advantage Chinese companies over U.S. and other non-Chinese companies. During its investigation into China's practices related to intellectual property and technology transfer, the Office of the United States Trade Representative determined the standards may require U.S. companies to make product or service-related disclosures that increase costs and/or risks.

Sources: McGregor, Morrison, OECD, Salidjanova et al., U.S.-China Economic and Security Review Commission, U.S. Chamber of Commerce, Office of the U.S. Trade Representative.

The U.S. Chamber of Commerce produced reports in 2016 and 2017 detailing trade policies between the United States and China, particularly as they relate to ICT products.[88] The shift in tone over the course of a year is revealing.

88 U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT* (Washington, DC: U.S. Chamber of Commerce, 2016), https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf; U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections* (Washington, DC: U.S. Chamber of Commerce, 2017), https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf.

The 2016 paper is cautiously optimistic that increasing trends to "deglobalize" trade could be reversed. The 2017 paper paints a darker view, seemingly more certain that China's course is increasingly set toward balkanization and creating disadvantages for foreign companies in support of domestic competitors and indigenous innovation.

These new regulations present a serious dilemma for U.S. multinationals and a threat to U.S. national security. If U.S. multinationals fail to adhere to Chinese government regulations, they may face restricted market access in China, which could decrease their revenues and global competitiveness. But if U.S. companies—which are the primary providers of ICT to the U.S. federal government—surrender source code, proprietary business information, and security information to the Chinese government, they open themselves and federal ICT networks to Chinese cyberespionage efforts.

This threat is not theoretical. Chinese government pressure on companies to submit source code for review may occur in support of, or in tandem with, other efforts to identify vulnerabilities in U.S. ICT products. The China Information Technology Evaluation Center (CNITSEC), which conducts the security reviews of foreign companies, is run by China's Ministry of State Security. But Recorded Future, a U.S.-Swedish internet technology company focusing on cyber intelligence, has linked CNITSEC to APT3, a China-based cyberespionage unit that has hacked federal agencies and companies in the United States and Hong Kong.[89]

Microsoft has allowed the Chinese government to access its source code since 2003, when it signed an agreement with CNITSEC allowing China to participate in its Government Security Program, which grants access to the source code and technical information of several versions of Windows software.[90] In January 2010, 34 U.S. companies, including Google, Adobe, Yahoo, and Northrop Grumman, were hit by attacks from China facilitated by a previously unknown vulnerability in Microsoft's Internet Explorer. In March 2010, researchers at McAfee claimed the January attacks targeted the companies' source-code management systems in an effort to extract proprietary source code.[91]

Reports from *The Guardian* indicate that the Microsoft source code used in the attacks was obtained from Chinese IT security companies. *The Guardian*'s reporting indicates CNITSEC and its partner, Topsec, may have passed Microsoft source code to the Chinese government units that carried out the hacking.[92] Topsec's connection to the Chinese government includes work related to China's space program, its national firewall, and other high-profile state projects, such as the 2008 Olympic Games, the 2010 World Expo, and the 2010 Guangzhou Asian Games.[93]

In October 2015, IBM became the first major U.S. tech company to allow officials from China's Ministry of Industry and Information Technology to examine its proprietary source code.[94] In September 2016, Microsoft announced the opening of its new Microsoft Transparency Center in Beijing, China, which will allow government officials to analyze and test products.[95] Additional Transparency Centers are located in Belgium, Brazil, Singapore, and the United States.[96]

89 Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," *Recorded Future* (blog), May 17, 2017, https://www.recordedfuture.com/chinese-mss-behind-apt3/; Mark Rockwell, "Feds Targeted in Clandestine Wolf Phishing Campaign," *FCW*, July 13, 2015, https://fcw.com/articles/2015/07/13/fed-phishing.aspx.

90 "Microsoft and China Announce Government Security Program Agreement," Microsoft, February 28, 2003, https://news.microsoft.com/2003/02/28/microsoft-and-china-announce-government-security-program-agreement/.

91 Kim Zetter, "Google Hackers Had Ability to Alter Source Code," *Wired*, March 3, 2010, https://www.wired.com/2010/03/source-code-hacks/.

92 Pascal-Emmanuel Gobry, "China Used Microsoft Source Code to Hack Google—And You?" *Business Insider*, December 7, 2010, http://www.businessinsider.com/wikileaks-china--microsoft-source-hack-google-2010-12.

93 "Introduction to TOPSEC," Topsec, http://www.topsec.com.cn/english/about_us.html.

94 Eva Dou, "IBM Allows Chinese Government to Review Source Code," *The Wall Street Journal*, October 16, 2015, https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

95 Scott Charney, "New Beijing Transparency Center Announced," Microsoft, September 19, 2016, https://blogs.microsoft.com/on-the-issues/2016/09/19/new-beijing-transparency-center-announced/.

96 "Government Security Program," Microsoft, June 2017, http://az370354.vo.msecnd.net/enterprise/GSP%20External%20Content%20Overview%20-%20Trust%20Center%20Version.pdf.

USING CHINESE COMPANIES TO FURTHER STATE GOALS

China is not a U.S. ally and is not likely to become one anytime soon. Moreover, the Chinese government and actors associated with it have repeatedly engaged in well-documented instances of theft and misuse of IP, as well as state-directed economic espionage. Chinese government policies summarized in **Table 4** are aimed at, among other goals, the creation and support of Chinese national champions—companies that further the government's strategic aims in return for government support.

Government support can take many forms, but it often includes preferential financing rates, preference in government contract bidding, and sometimes oligarchy or monopoly status in protected industries.[97] In the case of Chinese national champions, the support also appears to include officially sanctioned or officially conducted corporate espionage designed to improve the competitiveness of Chinese firms while potentially advancing other government interests.[98] Huawei, Zhongxing Telecommunications Corporation (ZTE), and Lenovo are three Chinese ICT companies that exhibit some of these characteristics.

Huawei is a Chinese multinational networking and telecommunications equipment company headquartered in Shenzhen.[99] Ren Zhengfei, a former officer in the People's Liberation Army (PLA) and a military technology researcher, founded Huawei in 1987 and continues to operate it.[100] Although Huawei is registered as a private company, a report by the U.S. House of Representatives Permanent Select Committee on Intelligence says Huawei:[101]

> *operates in what Beijing explicitly refers to as one of seven "strategic sectors." Strategic sectors are those considered as core to the national and security interests of the state. In these sectors, the CCP [Chinese Communist Party] ensures that "national champions" dominate through a combination of market protectionism, cheap loans, tax and subsidy programs, and diplomatic support in the case of offshore markets. Indeed, it is not possible to thrive in one of China's strategic sectors without regime largesse and approval.*

Huawei claims to be employee owned, but the company, unlike many Chinese corporations, has chosen not to sell shares in Hong Kong or the United States, which would require it to make financial disclosures.[102]

As early as 2000, hackers who appeared to be located in China infiltrated and exploited the networks of Nortel Networks Ltd., a foreign competitor of Huawei. Nortel was a multinational telecommunications and data networking equipment manufacturer headquartered in Canada. Nortel discovered the hacking in 2004 and determined that the hackers had obtained the passwords of seven top officials, including a previous CEO. Using China-based internet addresses, the hackers downloaded technical papers, R&D reports, and business plans, and monitored the employee email system.[103] The Nortel employee who conducted the internal investigation alleged that the hackers were based in Shanghai. Outside expert analysis determined that the rootkits installed on Nortel's systems were the work of professionals.[104]

---

97 Antonio Graceffo, "China's National Champions: State Support Makes Chinese Companies Dominant," *Foreign Policy Journal*, May 15, 2017, https://www.foreignpolicyjournal.com/2017/05/15/chinas-national-champions-state-support-makes-chinese-companies-dominant/.

98 Shane Harris, "Exclusive: Inside the FBI's Fight against Chinese Cyber-Espionage," Foreign Policy, May 27, 2014, http://foreignpolicy.com/2014/05/27/exclusive-inside-the-fbis-fight-against-chinese-cyber-espionage/; Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, *Testimony Before the House of Representatives Committee on Energy and Commerce Subcommittee on Oversight and Investigations* (July 9, 2013) (statement by Larry M. Wortzel), http://docs.house.gov/meetings/IF/IF02/20130709/101104/HHRG-113-IF02-Wstate-WortzelL-20130709-U1.pdf.

99 "Corporate Information," Huawei, accessed September 21, 2017, http://www.huawei.com/en/about-huawei.

100 Michael S. Schmidt, Keith Bradsher, and Christine Hauser, "U.S. Panel Cites Risks in Chinese Equipment," *The New York Times*, October 8, 2012, http://www.nytimes.com/2012/10/09/us/us-panel-calls-huawei-and-zte-national-security-threat.html.

101 Permanent Select Comm. on Intelligence, Investigative *Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE, a Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence*, U.S. House of Representatives, 112th Cong. (October 8, 2012), https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.

102 Schmidt, Bradsher, and Hauser, "U.S. Panel Cites Risks in Chinese Equipment."

103 Siobhan Gorman, "Chinese Hackers Suspected in Long-Term Nortel Breach," *The Wall Street Journal*, February 14, 2012, https://www.wsj.com/articles/SB10001424052970203363504577187502201577054.

104 Jameson Berkow, "Nortel Hacked to Pieces," *Financial Post*, February 25, 2012, http://business.financialpost.com/technology/nortel-hacked-to-pieces.

Nortel changed the compromised passwords, but six months later the hackers appeared to retain some access to the company's systems. Every month or so, a few computers on Nortel's network would send small bursts of data to one of the internet addresses in Shanghai involved in the password-hacking episodes. Subsequent investigations revealed that the hackers had installed spyware on Nortel's computers, could control some computers remotely, and had set up an encrypted communication channel to an internet address near Beijing. Nortel filed for bankruptcy in 2009. The hacking incident was not fully disclosed when the company began selling off assets, and reports from former Nortel employees indicate that firms such as Avaya, which acquired Nortel assets following the bankruptcy, may have inadvertently purchased compromised Nortel IT equipment, leaving Avaya's systems vulnerable to infiltration by the same hackers who targeted Nortel.[105] Unconfirmed reports suggest that the hackers who targeted Nortel (as well as Motorola and Cisco during the same period) were working on behalf of Huawei, which had surpassed its U.S. competitor, Cisco, in several core markets.[106]

Huawei has been the subject of numerous investigations and congressional hearings regarding the company's alleged ties to the Chinese Communist Party and the PLA.[107] In February 2011, the Committee on Foreign Investment in the United States issued a recommendation that Huawei voluntarily divest the assets it received in a 2010 deal with 3Leaf, a U.S. company that developed advanced computer technologies. In response, Huawei published an open letter to the U.S. government denying the existence of security issues in the company or its equipment and requesting a full investigation into its corporate operations.[108] The House Permanent Select Committee on Intelligence initiated an investigation into Huawei and ZTE in November 2011 and produced a report in October 2012. The following were among the report's recommendations:

- *U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts. Similarly, government contractors—particularly those working on contracts for sensitive U.S. programs—should exclude ZTE or Huawei equipment from their systems.*
- *Private sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence, and thus pose a security threat to the United States and to our systems.*[109]

Congressional concern with Huawei and ZTE has continued. In January 2018, U.S. Representative Mike Conaway (R-TX) introduced the Defending U.S. Government Communications Act, which would prohibit the U.S. government from purchasing and using "telecommunications equipment and/or services" from Huawei and ZTE.[110]

Huawei and ZTE are not the only Chinese companies to be accused of such activity. The Chinese computer and server manufacturer Lenovo is a similar case. Lenovo originally formed in 1984 as the New Technology Development Company, a component of the state-run Chinese Academy of Sciences Institute of Computing Technology.[111] The founder of Lenovo was educated at the Xi'an Military Communications Engineering Institution of the PLA, now Xidian University. The university has close connections with the PLA and is considered to be a link between China's civilian and military research on cybersecurity.[112] Additionally, Lenovo's CEO, who succeeded its

105 Tom Warren, "Hackers Roamed Nortel's Network for Years without Detection," *The Verge*, February 14, 2012, https://www.theverge.com/2012/2/14/2797047/nortel-undetected-hacking-breach.

106 Mark Anderson, "The Sony Hack and Nortel's Demise: Piracy vs. Crown Jewel Theft," *Forbes*, January 21, 2015, https://www.forbes.com/sites/valleyvoices/2015/01/21/the-sony-hack-and-nortels-demise-piracy-vs-crown-jewel-theft/#1efa1d54f0c9.

107 *Investigative Report on the U.S. National Security Issues*, U.S. House of Representatives.

108 Ken Hu, "Huawei Open Letter," *The Wall Street Journal*, February 5, 2011, http://online.wsj.com/public/resources/documents/Huawei20110205.pdf.

109 *Investigative Report on the U.S. National Security Issues*, U.S. House of Representatives.

110 Defending U.S. Government Communications Act, H.R. 34747, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/4747; Andrew Liptak, "A New Bill Would Ban the US Government from Using Huawei and ZTE Phones," *The Verge*, January 14, 2018, https://www.theverge.com/2018/1/14/16890110/new-bill-ban-huawei-zte-phones-tech-congress-mike-conaway-cybersecurity.

111 Nathaniel Ahrens and Yu *Zhou, China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan, CASE STUDY: Lenovo* (Washington, DC: Center for Strategic and International Studies, January 2013), https://www.csis.org/analysis/china%E2%80%99s-competitiveness-lenovo.

112 Edward Wong, "University in Xi'an Opens School of Cyberengineering," *Sinosphere: Dispatches from China* (blog), *The New York Times*, January 6, 2015, https://sinosphere.blogs.nytimes.com/2015/01/06/university-in-xian-opens-school-of-cyberengineering/.

founder, was educated at China's University of Science and Technology, which was established and resourced by the CAS.[113] The CAS and its individual members have a history of coordinating with the Chinese military, including its cyber and electronic warfare operations.[114] The Chinese government, through Legend Holdings Limited, is the largest shareholder of Lenovo stock. As of June 2017, the CAS (through CAS Holdings) owned 34.83 percent of Legend and was identified as Legend's controlling shareholder.[115] In 2017, Legend had 31.48 percent ownership in Lenovo.[116] Legend, which was formed by Lenovo's founder, operates as the external investment vehicle and asset management unit of the CAS.[117] Lenovo's growth has been attributed to the economic and political support it receives from the Chinese government, including the use of state-owned intellectual property resources.[118]

Lenovo has been linked to Chinese state-led cyberespionage efforts. Lenovo products have been banned by intelligence agencies in Australia, Canada, New Zealand, the United Kingdom, and the United States (Five Eyes Countries) since the mid-2000s, when laboratories of the British intelligence agencies Military Intelligence, Section 5 and Government Communications Headquarters discovered "backdoors"[119] and vulnerable firmware in Lenovo products.[120] In 2006, after congressional inquiries into the purchase of 16,000 Lenovo computers, the U.S. Department of State said the purchased computers would be used only on unclassified systems.[121] In 2015, the U.S. Navy announced it would replace servers for its guided missile cruisers and destroyers after Lenovo acquired certain IBM server and software product lines, due to concerns that the equipment could be compromised during maintenance or remotely accessed by the Chinese government.[122] In 2016, several incidents suggested the DoD may have banned Lenovo products owing to concerns about cyber spying against Pentagon networks and concerns that the company is installing backdoors in its products for the purposes of espionage. In April 2016, an Air Force email appeared to order that Lenovo products be removed from DoD networks. This message was subsequently retracted by Air Force and Pentagon spokeswomen.[123] In October 2016, *The Washington Free Beacon* reported that the Pentagon's Joint Staff had produced an internal report warning against using Lenovo equipment.[124]

In addition, Lenovo is believed to have been complicit in installing Superfish spyware and potentially a BIOS backdoor on a number of its computer products.[125] Superfish is a preloaded software shipped with Lenovo computers that ostensibly monitored internet browser traffic to improve advertisements, but also allowed hackers to read all encrypted browser traffic, including banking transactions, passwords, emails, and instant messages. The DHS U.S.

113 "USTC Introduction," University of Science and Technology of China, About, October 14, 2016, http://en.ustc.edu.cn/about/201101/t20110113_87798.html.

114 John Costello, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Intelligence Agencies: Reform and Future," June 9, 2016, http://www.uscc.gov/sites/default/files/John%20Costello_Written%20Testimony060916.pdf.

115 Legend Holdings, "Legend Holdings Corporation, 2017 Interim Report" (Hong Kong Stock Exchange, September 14, 2017), 45, http://www.hkexnews.hk/listedco/listconews/SEHK/2017/0929/LTN201709291285.pdf.

116 Factiva Database, Dow Jones and Reuters, New York.

117 Legend Holdings, "Legend Holdings Corporation, 2017 Interim Report," 30; Factiva Database, Dow Jones and Reuters, New York.

118 Ahrens and Zhou, *China's Competitiveness*.

119 A backdoor is a means of bypassing normal authentication or encryption in a computer system, product, or embedded device. A backdoor may be a hidden part of a program, a separate program, or code in the firmware of hardware or parts of an operating system.

120 Adi Robertson, "Lenovo Reportedly Banned by MI6, CIA, and Other Spy Agencies over Fear of Chinese Hacking (Update)," *The Verge*, July 30, 2013, https://www.theverge.com/2013/7/30/4570780/lenovo-reportedly-banned-by-mi6-cia-over-chinese-hacking-fears; Christopher Joye, Paul Smith, and John Kerin, "Spy Agencies Ban Lenovo PCs on Security Concerns," *Financial Review*, July 27, 2013, accessed via WayBackMachine, https://web.archive.org/web/20130729011053/http://www.afr.com/p/technology/spy_agencies_ban_lenovo_pcs_on_security_HVgcKTHp4bIA4ulCPqC7SL; Cahal Milmo, "MI6 and MI5 'Refuse to Use Lenovo Computers' over Claims Chinese Company Makes Them Vulnerable to Hacking," *Independent*, July 29, 2013, http://www.independent.co.uk/news/uk/home-news/mi6-and-mi5-refuse-to-use-lenovo-computers-over-claims-chinese-company-makes-them-vulnerable-to-8737072.html.

121 "US Government Restricts China PCs," *BBC News*, May 19, 2006, http://news.bbc.co.uk/2/hi/americas/4997288.stm.

122 Phil Muncaster, "US Navy Looks to Dump Lenovo Servers on Security Concerns–Report," I*nfosecurity Magazine*, May 7, 2015, https://www.infosecurity-magazine.com/news/us-navy-dumps-lenovo-servers/; Megan Eckstein, "Navy Needs New Servers for Aegis Cruisers and Destroyers after Chinese Purchase of IBM Line," *USNI News*, May 5, 2015, https://news.usni.org/2015/05/05/navy-needs-new-servers-for-aegis-cruisers-and-destroyers-after-chinese-purchase-of-ibm-line.

123 Hayley Tsukayama and Dan Lamothe, "How an Email Sparked a Squabble over Chinese-Owned Lenovo's Role at Pentagon," *The Washington Post*, April 22, 2016, https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html.

124 Bill Gertz, "Military Warns Chinese Computer Gear Poses Cyber Spy Threat," *The Washington Free Beacon*, October 24, 2016, http://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat/.

125 Vijay, "Lenovo PCs and Laptops Seem to Have a BIOS Level Backdoor," *TechWorm*, August 12, 2015, http://www.techworm.net/2015/08/lenovo-pcs-and-laptops-seem-to-have-a-bios-level-backdoor.html.

Computer Emergency Readiness Team issued an alert and mitigation details in response.[126] Users later discovered that Lenovo computers shipped with a rootkit-style covert installer that would reinstall unwanted software on computers after users had deleted it. In September 2017, Lenovo reached a settlement with the Federal Trade Commission over charges that the company harmed consumers. As part of the settlement, Lenovo is required to implement a comprehensive software security program for consumer software.[127] The security program will be subject to third-party audits.

TARGETING U.S. GOVERNMENT CONTRACTORS

The Chinese government and Chinese nationals have previously been linked to attempts to illegally obtain source code from U.S. ICT companies. Chinese actors, including those connected to the government, have a history of trying to obtain sensitive information about U.S. companies in order to exploit their networks, replicate their technologies, and outcompete them in the global marketplace. China-linked hacking has repeatedly targeted U.S. federal government entities and U.S. federal government contractors, including many key players in ICT contracting.[128]

In 2007, the FBI investigated Unisys after a dozen DHS computers that Unisys was supporting were compromised and significant amounts of unclassified but sensitive information was transferred to Chinese websites. It remains unknown precisely what information was removed.[129] In 2013, Bloomberg reported on China-linked hacking dating back to 2007 that targeted the North American arm of QinetiQ, a British satellite, drone, and software defense manufacturer.[130] QinetiQ supplies spy satellites, bomb disposal robots, and other products to the U.S. military. Through compromised QinetiQ networks, the hackers targeted the networks of NASA, U.S. rifle divisions, cybersecurity divisions, and databases related to the U.S. Army's Apache and Blackhawk helicopter fleet. According to *Bloomberg*, investigators attributed the attack to a group of Shanghai-based hackers nicknamed the "Comment Crew," a group linked by the cybersecurity firm Mandiant to PLA Unit 61398.[131]

China-linked hackers have also targeted RSA Security, a network security company that is a subsidiary of Dell. RSA's SecurID system is widely used by the U.S. government and its contractors for log-in security.[132] The most recent breach appears to have occurred in 2011, when a cyberattack on RSA Security led to data loss associated with RSA's SecurID system. In 2012, Gen. Keith Alexander, then director of the NSA and the head of U.S. Cyber Command, indicated in testimony before the Senate Armed Services Committee that RSA was a victim

126 Department of Homeland Security, "Lenovo Superfish Adware Vulnerable to HTTPS Spoofing," February 20, 2015, https://www.us-cert.gov/ncas/alerts/TA15-051A.

127 Federal Trade Commission, "Lenovo Settles FTC Charges It Harmed Consumers with Preinstalled Software on Its Laptops That Compromised Online Security," September 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/09/lenovo-settles-ftc-charges-it-harmed-consumers-preinstalled.

128 Hanqing Chen, "A Recent History of China's Cyber Attacks on the United States," *Pacific Standard*, September 4, 2014, https://psmag.com/environment/chinas-cyber-attacks-united-states-89919; "APT1: Exposing One of China's Cyber Espionage Units," Mandiant, February 18, 2013, https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; David E. Sanger, David Barboza, and Nicole Perlroth, "Chinese Army Unit Is Seen as Tied to Hacking Against U.S.," *The New York Times*, February 18, 2013, http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html; Michael S. Schmidt, David E. Sanger, and Nicole Perlroth, "Chinese Hackers Pursue Key Data on U.S. Workers," *The New York Times*, July 9, 2014, http://www.nytimes.com/2014/07/10/world/asia/chinese-hackers-pursue-key-data-on-us-workers.html; Brendan I. Koerner, "Inside the Cyberattack that Shocked the US Government," *Wired*, October 23, 2016, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/.

129 Mike Masnick, "FBI Investigating Unisys for Not Preventing US Gov't Computers from Getting Hacked," *Techdirt*, September 25, 2007, https://www.techdirt.com/articles/20070924/135824.shtml; Jason Mick, "Unisys Blamed for China-Connected Homeland Security Hacks," *DailyTech*, September 26, 2007, http://www.dailytech.com/Unisys+Blamed+for+ChinaConnected+Homeland+Security+Hacks/article9043.htm; Ellen Nakashima and Brian Krebs, "Contractor Blamed in DHS Data Breaches," *The Washington Post*, September 24, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/09/23/AR2007092301471.html; "Investigators: Homeland Security Computers Hacked," CNN, September 24, 2007, http://www.cnn.com/2007/US/09/24/homelandsecurity.computers/index.html.

130 Michael Riley and Ben Elgin, "China's Cyberspies Outwit Model for Bond's Q," Bloomberg, May 2, 2013, https://www.bloomberg.com/news/articles/2013-05-01/china-cyberspies-outwit-u-s-stealing-military-secrets; Michael Riley and Alex Tribou, "Hackers in China Compromise U.S. Defense Secrets," Bloomberg, May 2, 2013, https://www.bloomberg.com/graphics/infographics/hackers-in-china-compromise-us-defense-secrets.html.

131 "APT1: Exposing One of China's Cyber Espionage Units," Mandiant.

132 Elinor Mills, "China Linked to New Breaches Tied to RSA," CNet, June 6, 2011, https://www.cnet.com/news/china-linked-to-new-breaches-tied-to-rsa/.

of Chinese cyberespionage.[133] According to 2013 testimony by the executive chairman of RSA, the company detected a targeted cyberattack on its systems and recognized that product information had been extracted. RSA publicly disclosed the breach and alerted customers to help them mitigate the effects. The company took its own remediation steps, including replacing nearly all of the 40 million SecurID tokens in use.[134] Industry press reports indicate that RSA's reluctance to publicly disclose which data had been stolen during the breach may have led to breaches at other defense contractors, including Lockheed Martin, L-3 Communications, and Northrop Grumman.[135] In June 2011, Lockheed Martin confirmed that the breach it experienced was due to data stolen from RSA.[136]

In July 2013, researchers from Dell's SecureWorks unit identified hackers targeting an unnamed maker of audio-visual conference equipment.[137] The Dell researchers linked the hackers to the Chinese hacking group that breached RSA Security in 2011. Dell's researchers speculated the hackers were attempting to obtain source code of the company's products in order tap into boardroom and other high-level remote meetings. In December 2015, a former software engineer for IBM in China was arrested and charged with economic espionage and theft of trade secrets.[138] The engineer had stolen source code related to IBM's proprietary clustered file system, which facilitates faster computer performance, and attempted to share it with the PRC's National Health and Family Planning Commission.[139]

133 Kelly Jackson Higgins, "China Hacked RSA, U.S. Official Says," *Dark Reading*, March 29, 2012, https://www.darkreading.com/attacks-breaches/china-hacked-rsa-us-official-says/d/d-id/1137409; *Hearing on U.S. Strategic Command and U.S. Cyber Command, Testimony Before the Senate Armed Services* (March 27, 2012) (statement of Keith B. Alexander), 13, https://www.armed-services.senate.gov/imo/media/doc/12-19%20-%203-27-12.pdf.

134 Arthur W. Coviello, Jr., "Written Testimony before the U.S. Senate Committee on Commerce, Science & Transportation," June 25, 2013, https://www.emc.com/collateral/corporation/coviello-congressional-testimony-2013.pdf; Peter Bright, "RSA Finally Comes Clean: SecurID Is Compromised," *Ars Technica*, June 6, 2011, https://arstechnica.com/information-technology/2011/06/rsa-finally-comes-clean-securid-is-compromised/.

135 Elinor Mills, "Attack on RSA Used Zero-day Flash Exploit in Excel," CNet, April 5, 2011, https://www.cnet.com/news/attack-on-rsa-used-zero-day-flash-exploit-in-excel/; "Frequently Asked Questions about RSA SecurID: Information for RSA Customers," EMC, 2011, https://www.emc.com/collateral/guide/11455-customer-faq.pdf.

136 Christopher Drew, "Stolen Data Is Tracked to Hacking at Lockheed," *The New York Times*, June 3, 2011, http://www.nytimes.com/2011/06/04/technology/04security.html.

137 Joseph Menn, "Chinese Hackers Target Remote Conferencing Gear: Dell Researchers," Reuters, July 31, 2013, https://www.reuters.com/article/us-china-hacking/chinese-hackers-target-remote-conferencing-gear-dell-researchers-idUSBRE96U0YI20130731.

138 Nate Raymond, "Ex-IBM Employee from China Arrested in U.S. for Code Theft," Reuters, December 8, 2015, https://www.reuters.com/article/ibm-crime-china/ex-ibm-employee-from-china-arrested-in-u-s-for-code-theft-idUSL1N13X2LD20151208.

139 "Chinese National Charged for Stealing Source Code from Former Employer with Intent to Benefit Chinese Government," Department of Justice, June 14, 2016, https://www.justice.gov/opa/pr/chinese-national-charged-stealing-source-code-former-employer-intent-benefit-chinese.

Chapter 5: Closing Loopholes: Recommended SCRM Actions

Federal SCRM efforts have yet to be fully developed, and gaps in resources and processes continue to exist that allow procurement of high-risk technologies, or deployment of moderate- to low-risk technologies in ways that fail to mitigate supply chain risk. Given the budgetary challenges many federal agencies face, decisions are made on the basis of reducing cost in a way that inadvertently increases risk. Several paths could be taken to improve federal ICT supply chain security. Some involve legislative action, while others leverage federal acquisition authority.

The sections below describe four paths that should be evaluated as solutions to enhance federal ICT supply chain security, where a comprehensive solution will potentially implement more than one recommendation. Establishing a centralized leadership for SCRM, expanding legislative provisions related to SCRM, and promoting supply chain transparency are the most effective ways of improving federal ICT supply chain security, align with how industry thinks and functions, and will likely provide greater benefit and more public and private sector adoption than modifications to the role of NIST or other federal trade regulations.

ESTABLISHING CENTRALIZED LEADERSHIP FOR SCRM

Congress or the Executive Branch should (1) name the organization(s) charged with SCRM leadership, (2) provide specific resources for SCRM, and (3) encourage information sharing and consolidation of federal SCRM efforts. In the current SCRM ecosystem, responsibility for risk management is held at different levels within agencies, resulting in SCRM offices and efforts, such as those at NASA and the Departments of Energy, Commerce, and Defense, that function largely as under-resourced stovepipes, often lacking executive sponsorship or oversight, and catering to the needs and procurement policies of individual clients. Entities such as the DoD and the intelligence community maintain largely separate policies, many of which are not transparent or applicable to the broader federal government due to procurement practices and classification concerns, among other reasons. Additionally, these programs may be concerned with initial acquisition, rather than system lifecycle concerns.

Although the nature of commercial ICT means that the universe of potential suppliers serving the federal government is extremely large, SCRM analysis conducted at the GSA, Department of Energy, NASA, and Department of Commerce often covers the same set of ICT suppliers for different federal government clients. This duplication of effort is wasteful and unnecessary, and negatively affects U.S. national security posture through misspent resources and inconsistent activities. Congress or the Executive Branch could establish centralized leadership, as well as a function, to carry out baseline SCRM analysis for the entire federal government, freeing individual agencies to focus on unique suppliers and technologies and how the identified risks impact their programs. This entity would have to be resourced and staffed appropriately, and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering federal ICT networks.

The OMB should assign this authority—through modifications to Circular A-130—to the GSA, the DHS, or another federal agency that is often tasked with shared services. The GSA, which is already responsible for vetting and managing the federal government's relationship with more than 30,000 suppliers, would be a logical center of action for this effort. Given its government-wide procurement and acquisition mission, the GSA is capable of deciding what categories of risk this baseline level of analysis should include and what level of detail the analysis should pursue. It would be wise to cast as wide a net as possible, including both technical and security risks, as well as market and business risks. Funding such a venture to the point where it could create comprehensive and authoritative information would reduce the burden for agency-specific SCRM and enable agencies to build from the same foundation, focusing their efforts on particular configurations and implementation situations. Funding for this entity could include seed money as well as a cost-reimbursable model with the collaborating agencies.

However, basing a centralized SCRM effort in the GSA could present challenges. The GSA's mission is negotiating the best deal for the federal government in any procurement. Additionally, the GSA often contracts

with value-added resellers such as Mythics, DLT Solutions, Immix Group, Carahsoft, and CDW-G rather than with original equipment manufacturers (OEMs). There have been instances of OEMs (e.g., Oracle in September 2016) abandoning the GSA Schedule Contracts[140] because the effort to secure and maintain the contracts outweighed the benefits.[141] Dealing with value-added resellers rather than OEMs introduces additional risk into the federal ICT supply chain. Patrick Finn, a former senior vice president for Cisco, told Federal News Radio, "It's not uncommon for an OEM to be contacted by disgruntled customers who procured through GSA only to find out that the product was gray market or, worse, counterfeit."[142] Thus, placing SCRM for federal ICT in the hands of the GSA or any other federal agency could require not only financial and policy shifts but also cultural ones for both the government and industry. Financial cost is an element of SCRM analysis, but it should be weighed in context with security considerations.

Sharing SCRM information across the government must be done in an effective and transparent manner. The Department of Veterans Affairs (VA) has created the publicly accessible One-VA Technical Reference Module (TRM), which provides detailed information on technical risk assessments conducted by the One-VA TRM team, along with public decisions about the VA's investment or divestment in certain technologies. The TRM includes a public access site that provides TRM content, a VA internal access site that allows users to make inquiries and request technology assessments, and a TRM team collaboration site, which allows content authoring and Wiki-based development that can be pushed to published sites.[143] Users of the TRM can see when a technology was last assessed, what findings were recorded, and what actions and policies VA leadership has recommended in response to the TRM team's findings. Using a similar portal for SCRM, with distinct levels of public and government-only access, would be valuable to all federal SCRM efforts; it would prevent duplication of effort, save time, and enable agency-specific assessments to build from a common foundation and share their risk mitigation strategies. Additionally, by leveraging technology the government-wide sharing would be able to scale and sustain a robust program for all collaborating agencies.

EXPANDING THE WOLF PROVISION

Congress should expand legislative actions that address risk linked to the nature of an ICT manufacturer as well as the manufacturer's location. The Wolf Provision, or Section 516 (subsequently 515) of the 2013 Consolidated and Further Continuing Appropriations Act, is one example. This provision was added by then U.S. Representative Frank Wolf (R-VA), who chaired the House subcommittee that oversees the Departments of Commerce and Justice, NASA, and the National Science Foundation. Initially introduced in 2013, Section 516 prevented the Departments of Commerce and Justice, NASA, and the National Science Foundation from acquiring IT without first conducting a risk assessment. If the IT system was "produced, manufactured or assembled by one or more entities that are owned, directed or subsidized by the People's Republic of China" and the federal entity still wished to purchase it, then the entity had to explain to Congress why the acquisition was in the national interest of the United States.[144]

Although the Wolf Provision was criticized by industry and considered too specifically anti-China, the language of the original provision acknowledged that subjecting products to additional scrutiny purely on the basis of geographic location is not an effective course of action, especially when it comes to global ICT supply chains. The original call for scrutiny of products "produced, manufactured or assembled … by entities that are owned, directed or subsidized by the People's Republic of China," makes clear that the potential for risk does not depend solely on the manufacturing or assembly location of a product but rather on the nature of the entity overseeing production. The language of the provision was modified in 2014, and the current provision (now in Section 515 of the Appropriations Act) no longer specifically mentions China. Instead, it includes language drawn from the NIST publication FIPS 199, which requires risk assessments for high-impact or moderate-impact information

140 GSA Schedule Contracts, also known as GSA Schedules or Federal Supply Schedules, are indefinite delivery, indefinite quantity, long-term contracts under the GSA's Multiple Award Schedule Program.

141 Jason Miller, "Oracle to Leave GSA Schedule: A Signal of Broader Change?" *Federal News Radio*, September 26, 2016, https://federalnewsradio.com/reporters-notebook-jason-miller/2016/09/oracle-leave-gsa-schedule-signal-broader-change/.

142 Miller, "Oracle to Leave GSA Schedule."

143 Paul Tibbits, "DoD-VA Collaboration to Develop a Single Electronic Health Record: SOA as a Design Pattern," July 14, 2011, http://www.omg.org/news/meetings/workshops/SOA-HC/presentations-2011/14_FS-1_Tibbits.pdf.

144 Consolidated and Further Continuing Appropriations Act, 2013, H.R. 933, 113th Cong. (2013–2014), https://www.congress.gov/bill/113th-congress/house-bill/933/text.

systems. The current provision still applies only to the Departments of Commerce and Justice, NASA, and the National Science Foundation.[145]

Currently, no federal entities have all-encompassing risk assessment programs, nor are they directed to do so or be held accountable. The programs that do exist are not adequately resourced for effective implementation, and the fact that each agency interprets the requirements for itself means that SCRM practices can vary within—and between—federal agencies. Along with modifications to policy—such as Circular A-130—Congress should tie policy revisions to a funding strategy that ensures federal agencies take action in ways that are auditable. One recommendation is to expand the Wolf Provision, or Section 515 of the Consolidated and Further Continuing Appropriations Act, to apply to all federal agencies and entities. Another is to tie the SCRM requirements of this regulation to agency funding for the Modernizing Government Technology Act of 2017 in ways that require a SCRM program review for new ICT investments and modernization efforts. One improvement to the provision would be to require agencies to annually present information about (1) their established SCRM program, (2) the activities that have taken place within that program, and (3) the mitigations used. These annual reports will help build a best practices library for all federal government entities, increasing information sharing and awareness of evolving risks.

Another option is to modify the language in the Wolf Provision to direct extra scrutiny at products "produced, manufactured or assembled … by entities that are owned, directed or subsidized by" nation states or entities known to pose a potential supply chain or intelligence threat to the United States. These nation states or entities could include members of the existing Sensitive Foreign Nations Control List, the Office of the United States Trade Representative's Special 301 Report Priority Watch List, or some appropriate combination of the two.[146] This type of language would direct appropriate scrutiny at products produced by entities linked to the Chinese government, but would not place significant burden on ICT suppliers sourcing from other suppliers that may have some production facilities in China.

PROMOTING SUPPLY CHAIN TRANSPARENCY

Congress should encourage transparency and accountability for supply chains. Although this report addresses supply chains that intersect China, those are not the only sources of risk. The sheer magnitude of China's influence as a supplier and manufacturer, combined with sometimes undisclosed links between the Chinese government and Chinese firms, creates risk in federal ICT procurement. Requiring federal ICT suppliers to publish or make available information on their supply chain would increase the ability of the federal government to source responsibly and securely, and to respond to breaches in an efficient manner. The federal acquisition community could also be required to build supply chain transparency requirements or disclosures into ICT procurements for first- and second-tier suppliers, and then require that sub-tiers have this included in their flow-down clauses. Rather than seeking supply chain information from a company after an incident, the federal government and its industry partners would already have that information on hand. This information would allow the government to architect federal information systems accordingly, implement risk mitigation strategies as necessary, and trace potential weaknesses back to individual components and suppliers.

In testimony before the House Subcommittee on Communications and Technology in May 2013, Mark L. Goldstein, GAO director of physical infrastructure issues, reviewed findings from a GAO report regarding measures the governments of Australia, India, and the United Kingdom take to secure their ICT infrastructures.[147] India's licensing requirements include explicit supply chain measures such as requiring telecommunications service providers to keep a record of the supply chain for their hardware and software, and requiring suppliers to allow providers or government entities to inspect the supply chain. In the event of a security breach or an act of intentional omission, the Indian government can cancel the license of the provider and blacklist the vendor that supplied the

145 Consolidated Appropriations Act, 2017, H.R. 244, 115th Cong. (2017–2018), https://www.congress.gov/bill/115th-congress/house-bill/244/text.

146 "Attachment G Sensitive Foreign Nations Control," Department of Energy, 2014, https://energy.gov/sites/prod/files/2014/08/f18/alliance_partvII-g.pdf; Office of the United States Trade Representative, 2017 Special 301 Report (Washington, DC: Office of the United States Trade Representative, 2017), https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

147 *Telecommunications Networks: Addressing Potential Security Risks of Foreign-Manufactured Equipment, Testimony Before the House Subcommittee on Communications and Technology, Committee on Energy and Commerce* (May 21, 2013) (statement by Mark L. Goldstein), https://www.gao.gov/assets/660/654763.pdf.

hardware or software that caused the security breach.[148] This policy is similar to Section 806 authorities incorporated into the Defense Federal Acquisition Regulation Supplement (DFARS) as a final rule in October 2015.[149] Pursuing similar policies, or requiring federal contractors to provide supply chain information as part of federal contract requirements, would provide an additional layer of SCRM security when the program requires this level of rigor.

Dodd-Frank Limitations Are Future SCRM Lessons

There are challenges in significantly improving supply chain transparency, and important lessons can be learned from the experience of Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which aimed to reduce violence in the Democratic Republic of the Congo by limiting U.S. procurement from actors fueling conflict in the DRC. In addition to other consumer protection provisions, Section 1502 and the ensuing Securities and Exchange Commission (SEC) rules require some companies to document the use in their products of "conflict minerals" through SEC Specialized Disclosure (SD) filings and Conflict Mineral Reports.[150]

The corporate responsibility supplier lists issued by HP, Dell, and Microsoft provide information on the first tier of the federal ICT supply chain, but the SD filings and Conflict Mineral Reports provide information on the deepest tier, the ultimate source point of the raw material a vendor is using for its ICT products. Since the passage of Dodd-Frank Section 1502 and the publication of related SEC rules, companies have filed four rounds of SD filings with the SEC and reportedly invested four years in further investigating and performing due diligence on their supply chains. And yet failings and inconsistencies remain, highlighting the scope of the challenge.

The transparency introduced by Section 1502 and the SEC rules has forced companies to diligently investigate their own suppliers, many for the first time. The policy has also raised awareness of what responsible supply chain management and responsible sourcing entail. Early on, some companies chose not to source from central Africa as a way of avoiding conflict minerals, failing to realize that global supply chains mean that conflict minerals can end up in smelters in Belgium, China, Morocco, or the United Arab Emirates. This has clear parallels to global ICT supply chains, where components may pass through several countries before being incorporated into a final product.

As Dodd-Frank made clear, the threat to U.S. national security was not minerals sourced from the DRC and adjoining countries, but rather minerals sourced from mines controlled by parties to the DRC conflict. To scope this outward, the supply chain threat to U.S. national security is not merely from products manufactured in China, or even products manufactured by Chinese businesses, but rather from products produced, manufactured, or assembled by entities that are owned, directed, or subsidized by nation states or entities known to pose a potential supply chain or intelligence threat to the United States, of which China is one.

Recommendations for improving supply chain transparency with respect to conflict minerals are applicable to supply chain transparency more generally.[151] When scoped out to ICT supply chains, new reporting requirements could require companies to note the location of their suppliers' manufacturing centers, and to identify which manufacturing centers are located in nation states known to pose a potential supply chain or intelligence threat to the United States. If a company cannot identify its suppliers' manufacturing locations, or if the location it reports appear inaccurate, it could be a warning sign that their SCRM program is not sufficient to protect the security concerns of the U.S. government.

148 *Telecommunications Networks* (Goldstein).

149 Susan Borschel, "New Department of Defense Requirements Relating to Supply Chain Risk," *Government Contracting Insights*, November 13, 2015, http://govcon.mofo.com/national-security/new-department-of-defense-requirements-supply-chain-risk/.

150 Conflict minerals are defined by U.S. legislation and SEC rules as the four metals tantalum, tin, tungsten, and gold. Tantalum, tin, and tungsten are the derivatives of the minerals columbite-tantalite (coltan), cassiterite, and wolframite, respectively. Many of these metals are sourced from the Democratic Republic of the Congo or adjoining countries. The most common conflict minerals are casserite (tin), coltan (tantalum), wolframite (tungsten), and gold, which are often collectively termed "3TG."

151 Jeff Schwartz, "The Conflict Minerals Experiment," *Harvard Business Law Review 6* (January 2015), https://ssrn.com/abstract=2548267 or http://dx.doi.org/10.2139/ssrn.2548267; *Testimony Before the House Subcommittee on Monetary Policy and Trade, Committee on Financial Services* (November 17, 2015) (statement by Jeff Schwartz), https://financialservices.house.gov/uploadedfiles/hhrg-114-ba19-wstate-jschwartz-20151117.pdf.

UTILIZING FEDERAL ACQUISITION AUTHORITIES

The final recommendation to enhance SCRM is to use the purchasing power of the U.S. government to require commercial suppliers to meet certain cybersecurity and SCRM standards to be eligible for federal contracts.[152] This option would make SCRM issues a priority for all industry partners interested in competing for government contracts, raising their level of security before they even have access to sensitive federal information. Increasing the security posture of entities before they become a target could help them defend themselves, and the federal government, against attacks from actors linked to China.

Federal contracts could use acquisition methods, including contract clauses and flow-down requirements, to require contractors and subcontractors to meet such standards. The federal government must be clear about the risk concerns and thresholds so that industry can clearly understand, based on each program, where to include SCRM investments. Although a minimum level of SCRM should be documented, not every procurement will identically use a product or service. A strict and inflexible requirement for every acquisition and supplier to undergo the maximum level of SCRM activities will be costly and unworkable.

One example of this approach is DFARS regulations on unclassified controlled technical information and controlled unclassified information, categories of information that are considered sensitive but are not classified and regulated by the federal government. These regulations require contractors to implement specific security measures in accordance with NIST SP 800-171, including access control, training, system audit records to monitor system activity, media protection and disposal, and other requirements. These measures are a necessary step, but may not mitigate the risk posed by ICT components produced in China or by entities linked to the Chinese government. NIST SP 800-171 took effect on December 13, 2017, for the DoD, the GSA, and NASA.[153]

Meanwhile, through their joint authority, the DoD, the GSA, and NASA are proposing a similar Federal Acquisition Regulation clause for contractors that handle, possess, use, share, or receive controlled unclassified information for other federal agencies.[154] This rule would have a similar effect as the DFARS and is an example of another way NIST recommendations can become obligatory.

152 Robert S. Metzger, "Threats to the Supply Chain: Extending Federal Cybersecurity Safeguards to the Commercial Sector," Bloomberg Law, June 8, 2015, https://www.bna.com/threats-supply-chain-n17179927448.

153 Matt Kozloski, "Everything You Need to Know about NIST 800-171," Kelser, December 16, 2016, https://inbound.kelsercorp.com/blog/everything-you-need-to-know-about-nist-800-171.

154 Undersecretary of Defense for Acquisition, Tech. and Logistics, "Open FAR Cases as of 10/31/2017," Department of Defense, accessed October 31, 2017, http://www.acq.osd.mil/dpap/dars/opencases/farcasenum/far.pdf; "Federal Acquisition Regulation (FAR); FAR Case 2017-016, Controlled Unclassified Information (CUI)," Office of Information and Regulatory Affairs, Office of Management and Budget, accessed October 31, 2017, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201704&RIN=9000-AN56.

Chapter 6: Future Considerations

As stated at the beginning of this report, the attacks on U.S. federal ICT networks will only grow as the attack vectors—and the speed with which they can be reached—increase.

As the U.S. government develops enhanced SCRM policies and regulations, it is imperative to understand—and have a strategy to address—the risk developing technologies may pose to federal ICT systems. The Chinese government and Chinese companies have developed joint strategies to influence future developments to the advantage of Chinese ICT products. China's role in setting international technology standards is likely to increase, and similar strategies are likely to be used in the future in fields beyond ICT, such as pharmaceuticals, biotechnology, medical technology, nanotechnology, virtual reality, and artificial intelligence. With China's focus on proactive measures, the United States should adopt the same forward-leaning posture focused on security.

Increasingly, the importance of an ICT component's physical structure pales in comparison with the firmware and software operating within in it. In 2016, researchers from Red Balloon Security identified vulnerabilities that allowed hackers to surveil and manipulate users by hacking the embedded firmware of computer monitors.[155] In 2017, researchers uncovered vulnerabilities in HP, Dell, and Lexmark printers that allowed attackers to steal passwords, shut down printers, and even reroute print jobs.[156] The mid-2017 CCleaner supply chain attack, in which hackers accessed the code development structure of Piriform in order to install malware into the company's Windows utility product, typifies the types of threats federal ICT systems will continue to face. Over 2.2 million users downloaded CCleaner and unwittingly downloaded the hacker's embedded malware at the same time. This malware compromised 40 international technology firms, 51 international banks, and at least 540 computers connected to various governments.[157] Firms targeted by the hackers included many within the federal ICT ecosystem, including Cisco, Google (Gmail), Microsoft, Intel, Samsung, Sony, HTC, VMware, Vodafone, Epson, and Oracle.[158] The federal government's ability to identify risks, to protect federal information systems, and to respond to and recover from attacks and breaches hinges on developing a comprehensive understanding of the supply chain risk.

Other aspects of supply chain risk depend on technologies that are not yet developed or deployed, such as 5G mobile network technology, which is expected to start deploying in 2020. 5G is important for subsequent developments in virtual reality, artificial intelligence, and seamless integration of the Internet of Things.[159] The full deployment of 5G networks is expected to dramatically expand the number of connected devices, reduce network energy use, and decrease end-to-end round-trip delay (latency[160]) to under one millisecond.[161] Although the finalization of 5G

155 Franceschi-Bicchierai, "Hackers Could Break into Your Monitor."

156 Tom Spring, "Flaws Found in Popular Printer Models," *Threat Post*, January 31, 2017, https://threatpost.com/flaws-found-in-popular-printer-models/123488/.

157 Lucian Constantin, "Researchers Link CCleaner Hack to Cyberespionage Group," *Motherboard*, September 21, 2017, https://motherboard.vice.com/en_us/article/7xkxba/researchers-link-ccleaner-hack-to-cyberespionage-group.

158 India Ashok, "CCleaner Hack: Chinese Hacker Group Axiom May Have Carried out Attack to Target Major Tech Giants," *International Business Times*, September 21, 2017, http://www.ibtimes.co.uk/ccleaner-hack-chinese-hacker-group-axiom-may-have-carried-out-attack-target-major-tech-giants-1640208; Catalin Cimpanu, "Avast Publishes Full List of Companies Affected by CCleaner Second-Stage Malware," *Bleeping Computer*, September 25, 2017, https://www.bleepingcomputer.com/news/security/avast-publishes-full-list-of-companies-affected-by-ccleaner-second-stage-malware/; Dan Goodin, "CCleaner Backdoor Infecting Millions Delivered Mystery Payload to 40 PCs," *Ars Technica*, September 25, 2017, https://arstechnica.com/information-technology/2017/09/ccleaner-backdoor-infecting-millions-delivered-mystery-payload-to-40-pcs/.

159 Sebastian Moss, "ITU and Huawei Call for Government-backed Broadband Investment," Data Center Dynamics, October 7, 2016, http://www.datacenterdynamics.com/content-tracks/core-edge/itu-and-huawei-call-for-government-backed-broadband-investment/97066.fullarticle.

160 Latency refers to the delay before a transfer of data begins following an instruction for its transfer. Decreasing latency to under one millisecond is seen as vital to successfully developing safe self-driving vehicles and producing virtual reality programs that can deliver data at a rate that feels near-instantaneous to humans.

161 Jo Best, "The Race to 5G: Inside the Fight for the Future of Mobile as We Know It," TechRepublic, https://www.techrepublic.com/article/does-the-world-really-need-5g/.

standards may be years away, Chinese entities (specifically Huawei and ZTE) have made large strides in patenting ICT innovations, so China could emerge as an industry leader in this technology.[162]

In 2016, the United States ranked first in patent filings for the 39th year in a row.[163] However, China's efforts to expand its ownership of IP are increasing; if this trend continues, China could overtake the United States in two years as the largest user of the international Patent Cooperation Treaty system. According to data from the World Intellectual Property Organization, Huawei and ZTE (along with Qualcomm) have been the top three patent filers each year since 2012.[164]

It is difficult to use patent and other IP data as a measure of a country's innovation because of differences in the policies of national patent offices and the inherent challenge of weighing the influence of any one IP application. It is also difficult to ascertain in advance which IP claims are essential to standards and which will win out when subjected to litigation. The Center for International and Strategic Studies argues that context is necessary when using patents to measure China's innovation.[165] The National Patent Development Strategy of China's State Intellectual Property Office explicitly equates patent generation with innovation. To encourage companies to file patents, the Chinese government offers incentives such as cash bonuses, subsidies, and lower corporate income taxes. This strategy might encourage quantity over quality, so that some State Intellectual Property Office patents are awarded for incremental innovations and design modifications rather than dramatic innovations.

Moreover, large increases in domestic patent filings in China have not translated into large increases in the number of triadic patents, which are patents filed jointly in the three largest global technology markets: the Japanese Patent Office, the U.S. Patent and Trade Office, and the European Patent Office. The Center for International and Strategic Studies notes, "While China now processes the greatest number of domestic patent applications annually, these patents do not hold up under the more stringent requirements of the international patent system."[166] Additionally, Chinese patent applications are not spread widely among Chinese firms but rather are concentrated in the hands of government-backed ICT firms such as Huawei and ZTE.

The Chinese government and Chinese firms are hoping for a larger stake in the new 5G developments than they had in 3G and 4G-LTE.[167] Of the 4,123 patents that ZTE applied for in 2016, more than 1,500 are 5G-related.[168] Huawei's 5G research dates to 2009 and includes advances in polar coding and network splicing routers. Huawei has also bought technology patents from Sharp, IBM, Siemens, Harris Corporation, and other U.S., Japanese, and European companies. These patent acquisitions focus on communication technologies such as the Session Initiation Protocol.[169]

A March 2017 report by LexInnova laid out the major players in the 5G network technology IP landscape.[170] **Exhibit 4** shows share of 4G-LTE and 5G IP among top firms. Qualcomm, Nokia, InterDigital, Ericsson, Intel, and Huawei are the top six firms for 5G IP. Qualcomm, Samsung, Intel, Ericsson, Nokia, and LG were the top six firms for

162 Ben Sin, "How Huawei Is Leading 5G Development," *Forbes*, April 28, 2017, https://www.forbes.com/sites/bensin/2017/04/28/what-is-5g-and-whos-leading-the-way-in-development/#1d015f0e2691.

163 World Intellectual Property Organization, "Record Year for International Patent Applications in 2016; Strong Demand Also for Trademark and Industrial Design Protection," press release, March 15, 2017, http://www.wipo.int/pressroom/en/articles/2017/article_0002.html.

164 World Intellectual Property Organization, "U.S. Extends Lead in International Patent and Trademark Filings," press release, March 16, 2016, http://www.wipo.int/pressroom/en/articles/2016/article_0002.html; World Intellectual Property Organization, "Telecoms Firms Lead WIPO International Patent Filings," press release, March 19, 2015, http://www.wipo.int/pressroom/en/articles/2015/article_0004.html; World Intellectual Property Organization, "US and China Drive International Patent Filing Growth in Record-Setting Year," press release, March 13, 2014, http://www.wipo.int/pressroom/en/articles/2014/article_0002.html; World Intellectual Property Organization, "Strong Growth in Demand for Intellectual Property Rights in 2012," press release, March 19, 2013, http://www.wipo.int/pressroom/en/articles/2013/article_0006.html.

165 China Power Team, "Are Patents Indicative of Chinese Innovation?" China Power, February 15, 2016, updated August 11, 2017, https://chinapower.csis.org/patents/.

166 China Power Team, "Are Patents Indicative of Chinese Innovation?"

167 4G-LTE, or long-term evolution, is a telecommunication standard for high-speed wireless communication for mobile devices and data terminals.

168 Saleha Riaz, "ZTE, Huawei Top Patent Application Table in 2016," *Mobile World Live*, March 16, 2017, https://www.mobileworldlive.com/featured-content/top-three/zte-huawei-top-patent-application-table-in-2016/.

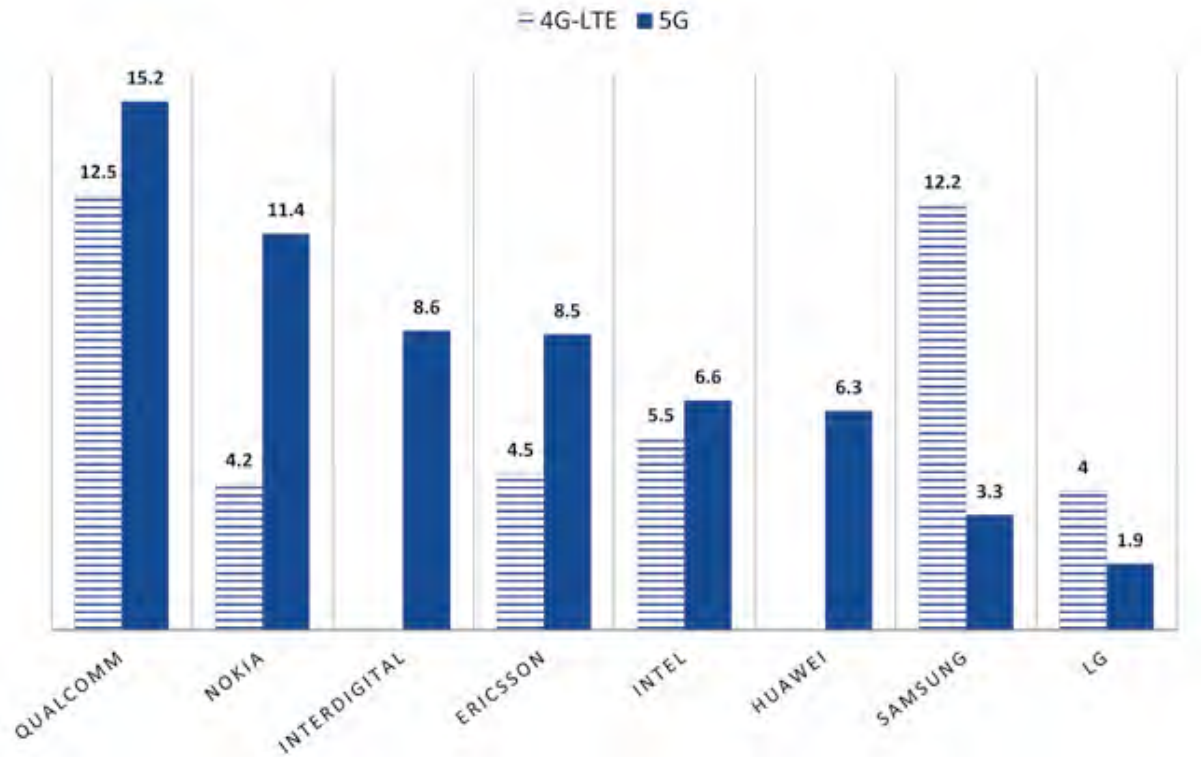
169 Jack Ellis, "A Peek Inside Huawei's Shopping Basket Reveals How Patent Purchases Further Its Expansion Plans," IAM, May 7, 2015, http://www.iam-media.com/Blog/Detail.aspx?g=0351e5a1-3675-43a9-a552-7c8206af6be3.

170 "5G Mobile Network Technology: Patent Landscape Analysis," LexInnova, March 15, 2017, http://www.lex-innova.com/resources-reports/?id=67.

4G-LTE IP. Many of the top firms from 4G-LTE development remain competitive in the 5G sphere, with Qualcomm continuing to lead the group, and Nokia, Ericsson, and Intel increasing their share of relevant IP rights in 5G with respect to 4G-LTE. Although Samsung was a close second to Qualcomm in 4G-LTE innovation, it has fallen to 10th in 5G IP, according to the LexInnova data. LG has similarly struggled, losing influence in 5G innovation to its competitors. Newly important players include InterDigital (a nonparticipating U.S. entity that owns IP but does not produce products) and Huawei.

Exhibit 4

Percent Share 4G-LTE and 5G Wireless Network IP Rights by Firm



Sources: LexInnova, iRunway, Jefferies.

According to the LexInnova data, Huawei may control as much as 6.3 percent of critical 5G mobile network technology IP, a shift from its lack of influence in 4G-LTE. All Chinese entities together (including contributions from Huawei, ZTE, the China Academy of Telecommunications Technology, Zhejiang University, and Lenovo Group) control 9.8 percent of the IP LexInnova deemed critical to the 5G standard. Chinese firms have the largest presence in the Radio Front End/Radio Access Network category, where Huawei has 41 patents, China Academy of Telecommunications Technology has 14, ZTE has 11, and Zhejiang University has 10. In the area of Modulation/Waveforms, Huawei has 27 patents, while Lenovo Group has 7. In the area of Core Packet Networking Technologies, Huawei has 24 patents and ZTE has 8. However, Chinese entities still lag behind ICT powerhouses such as Ericsson, Qualcomm, and Nokia, which represent the bulk of 5G-related patent holders.[171] The LexInnova report notes that the presence of Chinese entities among the top IP assignees may indicate that China's 5G deployment timeline is similar to that of the United States.

The creation of 5G standards is divided into two phases. Phase 1 will be finalized by the end of 2017; it is a soft transition phase to 5G that involves backward compatibility with 4G-LTE to protect legacy investments. Phase 2 will be finalized in mid-2018 and will introduce significant changes. Key decisions on these standards will be made in international organizations such as the International Telecommunication Union (ITU) and the Third Generation Partnership Project (3GPP). The ITU is a specialized agency of the United Nations responsible for ICT issues; the 3GPP is a collaborative organization among telecommunications associations. In both arenas, China has sought

171 Guy Daniels, "If You Thought Patents Got Ugly with LTE, Just Wait until 5G," *Telecom TV*, http://www.telecomtv.com/articles/5g/if-you-thought-patents-got-ugly-with-lte-just-wait-until-5g-13458/.

leadership positions to increase its influence. In the 3GPP, China has been represented by members of Huawei and China Mobile. In October 2014, Houlin Zhao was elected secretary general of the ITU.[172] His four-year term began January 1, 2015, and concludes at the end of 2018. In October 2016, Huawei's Site Energy Efficiency proposal was approved by the ITU.[173] The 3GPP has also accepted Huawei-backed polar code as the coding method for the control channel for 5G Phase 1,[174] and Chinese companies have several proposals in play for Phase 2.[175]

172 "Biography—Houlin Zhao," International Telecommunication Union, 2017, http://www.itu.int/en/osg/Pages/biography-zhao.aspx; Xinhua, "China's Zhao Houlin Elected as Secretary-General of ITU," *China Daily USA*, October 23, 2014, http://usa.chinadaily.com.cn/world/2014-10/23/content_18791007.htm.

173 "Huawei's SEE Becomes International Standard after ITU Approval," Huawei, December 5, 2016, http://www.huawei.com/en/news/2016/12/Huawei-SEE-International-Standard-ITU.

174 Louise Lucas and Nic Fildes, "Huawei Aims to Help Set 5G Standards," *Financial Times*, November 29, 2016, https://www.ft.com/content/f84f968c-b45c-11e6-961e-a1acd97f622d.

175 Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," Jefferies Hong Kong Limited, September 14, 2017. http://pdf.zacks.com/pdf/JY/H5194437.PDF.

Conclusions

It is unlikely that political or economic shifts will push global ICT manufacturers to dramatically reduce their operations in China or their partnerships with Chinese firms. A national strategy is needed for supply chain risk management of U.S. ICT, and it must include supporting policies so that U.S. security posture is forward-leaning, rather than reactive and based on incident response.

To successfully manage risks associated with Chinese-made products and services and the participation of Chinese companies in ICT supply chains, the U.S. government should:

- ***Establish Centralized Leadership for SCRM***: Threats to U.S. national security posed by state-directed or state-backed adversaries targeting U.S. federal ICT systems will continue, and China's role is in global ICT supply chains is unlikely to change in the near future. In a constrained resource environment, the federal government will need to have a strategy that focuses policy on those threats and vulnerabilities that have the greatest likelihood of occurrence. Establishing a technology-enabled shared SCRM services capability that all federal agencies can access is likely the most cost-effective and impactful means for tackling this evolving threat. A centralized entity for SCRM would need executive-level sponsorship, to be resourced and staffed appropriately and tasked with vetting to a prescribed level the suppliers and value-added resellers of products entering the federal IT network. This entity's work should be unclassified, but the entity should have a relationship with the intelligence community to ensure collaboration and information sharing.

- ***Embrace an Adaptive SCRM Process***: Federal ICT modernization efforts mean that new products entering the federal information systems and NSS have increasingly complex and globalized supply chains, many of which include commercial suppliers that source from China. These supply chains will change over time as companies develop new technologies and partner with new suppliers, and effective SCRM policies must be able to adapt as well. Policymakers must empower rather than hinder the efforts of successful collaborative entities such as NIST and keep as much discussion of the supply chain threat as possible in the unclassified public sphere.

- ***Promote Supply Chain Transparency***: The government should encourage the public exposure of primary or tier-one suppliers to federal ICT providers and should push for transparency of all suppliers where necessary for certain systems or suppliers at a particular risk or impact level. Suppliers should be required to be transparent about their relationships with entities that are owned, directed, or subsidized by nation states like China, or other entities known to pose a potential supply chain or intelligence threat to the United States. The government should have mechanisms in place and reward industry engagement with these efforts, while establishing consequences for failure to mitigate risk exposure.

- ***Prioritize SCRM throughout the Lifecycle of a Program***: The federal acquisition community should build supply chain transparency requirements or disclosures into ICT procurements from "birth to demise." Having supply chain information on hand earlier and until the end of the program will allow the government to architect federal information systems accordingly, implement risk mitigation strategies as necessary, and trace potential weaknesses back to individual components and suppliers while the program is operational.

- ***Have a Strategy and Craft Froward-Looking Policy***: Next-generation technologies and standards will have implications for U.S. national security in ways that may not be addressed by existing policies and regulations. Identifying future supply chain risks and addressing them creatively will be important to the success of federal policy efforts. Future risks will likely involve software, cloud-based infrastructures, and hyper-converged products rather than hardware. A vendor's, supplier's, or manufacturer's business alliances, investment sources, and joint R&D efforts are also sources of risk not always addressed in traditional SCRM.

Having a strategy that includes these steps will ensure that new SCRM policies can be adaptive, be collaborative, and achieve buy-in from both government and industry. Increased transparency will enhance the security of the federal ICT supply chain by enabling the federal government to source responsibly and securely, and by improving the government's ability to respond to incidents in the event of a supply chain attack, while centralization will reduce the burden facing agency-specific SCRM and allow agencies to focus their efforts on particular configurations and implementation situations. Moreover, building supply chain security into policy from the beginning will prevent costly mitigation later, and ensure that federal ICT supply chains—and the federal information systems they supply—remain secure.

Scope Note

This paper is an unclassified report on commercial supply chain vulnerabilities in U.S. federal ICT procurement linked to the People's Republic of China. The study was requested by the U.S.-China Economic and Security Review Commission and is intended as a reference for policymakers, China specialists, and supply chain professionals on how the U.S. government manages risks associated with Chinese-made products and services and the participation of Chinese companies in U.S. ICT supply chains. The research for this project covered three major connection routes between China and U.S. federal ICT supply chains and the risks those connections pose to U.S. national security. Sources used in this paper may refer to information technology, which can include computers, software, electronics, and other information distribution technologies. This paper's scope addresses the more expansive category of ICT, which encompasses audio-visual communications systems, data storage, and other integration technologies.

METHODOLOGY

This study defines "U.S. government ICT supply chains" as (1) primary suppliers, (2) tiers of suppliers that support primary suppliers by providing products and services, and (3) any entities linked to those tiered suppliers through commercial, financial, or other relevant relationships. This comprehensive definition includes supply chains that are multi-tiered, webbed relationships in addition to those that are singular or linear in nature. The greatest risk is often found in the second or third tiers of a supply chain and in indirect relationships within the chain.

The Commission requested a study that reviewed laws, regulations, and other requirements since the passage of FITARA in February 2014. The study includes detailed recommendations to minimize the risk that the Chinese government, Chinese companies, or Chinese products may pose to U.S. federal ICT supply chains. Interos supply chain risk analysts and China experts were specifically tasked by the Commission to assess—

1. China's role in the global ICT supply chain and China's participation in U.S. federal ICT supply chains, including U.S. government reliance on Chinese firms, products, and services and the risk those products and services pose to U.S. economic health and national security
2. Cases in which the Chinese government, Chinese companies, or Chinese products have been implicated in connection with U.S. supply chain vulnerabilities or exploitation
3. Current U.S. government efforts to manage risk from foreign-made products and foreign firms participating in its IT procurement, including differences between non-national-security-related and national-security-related ICT procurement
4. Points of vulnerability and loopholes in the existing U.S. federal risk management system, including prospects for future development as Chinese manufacturing, research, and development capabilities evolve

Included in this report are seven of the largest providers of enterprise IT to the U.S. federal government that are also ICT OEMs: HP, IBM, Dell, Cisco, Unisys, Microsoft, and Intel.[176] This is not to say these are the only companies with potential challenges in their supply chains, and it should be noted that none of these companies were approached as part of this report. Although all of these companies conduct some level of due diligence on their supplier base, their complete records are not publicly available.

176 "Top 25 Enterprise IT Providers," FedScoop.

SOURCES

The source material for this study is unclassified, publicly available, open source information, to include information from media, the internet, public government data, academic and industry publications, and commercial databases. For some subjects, the implications of unclassified information are highly suggestive yet inconclusive. For example, unclassified information is often insufficient to conclusively attribute ICT network intrusions and telecommunications supply chain vulnerabilities to the Chinese government, Chinese companies, or Chinese products. The analysis and attributions in this study present the best available unclassified information, with appropriate caveats when necessary.

The Chinese source material for the study came from authoritative PRC publications and authors, including government-affiliated press entities, and from the Chinese- and English-language web pages of Chinese companies, including defense providers and ICT suppliers.

Additional data used in the supply chain analysis of major U.S. federal ICT suppliers were obtained from relevant open source intelligence, including social media, free and subscription services, and other structured and unstructured data sources.

The result is a comprehensive review of the links between major U.S. federal ICT suppliers and the Chinese government, Chinese companies, and Chinese products that may pose a risk to U.S. federal ICT supply chains.

Acknowledgments

Interos Solutions would like to thank the U.S.-China Economic and Security Review Commission for its support of this research and the opportunity to present these findings. That said, we could not have produced this report without help from others. Our thanks are also due to Tara Madison, Sheila Gagen, Johanna Daproza, and other members of Vector Talent Resources for their editorial and design support.

Exhibit 15

10/11/2019 Huawei Ex Parte
(providing an expert report analyzing the economic impact of excluding Huawei from the U.S. market)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket.

Huawei submits as **Attachment 1** the expert report of economist Dr. Debra J. Aron[1] analyzing the impact of excluding Huawei from the U.S. market. As the Commission is well aware, a substantial number of carriers receive some form of Universal Service Fund ("USF") support from the Commission, as do many public schools, libraries, and vendors providing e-Rate-supported services.[2] The proposed rule would prohibit Huawei from providing equipment or services to any of these carriers, who collectively account for a significant segment of the U.S.

---

[1] *See* Debra J. Aron, "The Impact on the U.S. Economy of Excluding Huawei from Participation in the U.S. Market for Wireless Network Equipment," CHARLES RIVER ASSOCIATES (Oct. 7, 2019) ("Aron Report").

[2] *See Universal Service Monitoring Report*, CC Docket No. 96-45 *et al.*, Table 1.10, p. 19 (2018) (providing for $8.882 billion in USF claims for the High-Cost, Lifeline, Rural Health Care and E-Rate programs in 2017).

telecommunications market. In addition, as Huawei has already noted in the record, the stigma created by the proposed rule would discourage telecommunications carriers, both large and small, from purchasing equipment manufactured by Huawei beyond those that receive grants from the federal USF, further limiting the company's ability to participate in the U.S. market.[3] Thus, the proposed rule, as written, would have the practical effect of excluding Huawei from the U.S. telecommunications infrastructure market entirely. Additionally, barring Huawei from the U.S. market would harm the U.S. economy by delaying 5G deployment and impeding competition, resulting in both decreased employment and increased costs that will inevitably be borne by U.S. consumers. Dr. Aron's report provides the Commission with important economic data illustrating the deleterious impact that excluding Huawei from the U.S. market will have as the U.S. transitions its wireless infrastructure to support 5G technology and the services that it enables.

First, Dr. Aron details the United States' lagging position in 5G deployment as compared with the progress other countries have made. Huawei's absence from the U.S. market will only exacerbate the disparity between deployment of 5G networks in the United States and deployment of 5G networks in countries that do not bar Huawei from participating in the market. To close this gap, the United States must deploy the best telecommunications equipment available and encourage a competitive telecommunications equipment marketplace. Excluding Huawei is contrary to both of those goals. For instance, radio access network ("RAN") equipment is a crucial component of 5G networks. But, there are currently only five vendors that have the capacity to provide 5G RAN equipment to the international telecommunications marketplace at the scale that

---

[3] *See* Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89 (June 1, 2018), at pp. 57-59.

will be required to support pervasive 5G deployment. As Dr. Aron demonstrates, Huawei is a market leader in the development of 5G technology and standards as a result of its significant investment in research and development.[4] Huawei's products have earned numerous industry accolades. Huawei's 5G technologies and equipment capabilities are estimated to be as much as 12-24 months more advanced than those of its competitors'. Those products include key equipment such as Massive MIMO (multiple input, multiple output) antennas, which are critical to 5G RAN deployment.

Second, Dr. Aron examines the impact of delayed 5G deployment on the U.S. economy and the established relationship between telecommunications technology—in particular, mobile broadband technology—and gross domestic product ("GDP"). The Commission has consistently recognized that "5G is critical to [the U.S.] economy, security and quality of life . . . ."[5] Accenture projects that the direct economic benefits associated with 5G will be substantial – "U.S. telecom operators could invest approximately $275 billion over seven years to deploy next-generation wireless technology[,]" could result in the creation of 3 million jobs, and may result in GDP growth of approximately $500 billion.[6] Studies illustrate that delays in technology penetration dampen GDP growth.[7] Expedient 5G deployment, in contrast, would directly benefit the U.S. economy by

---

[4] *See* Aron Report at Section VII.A

[5] Remarks of FCC Chairman Ajit Pai, National Spectrum Consortium 5G Collaboration Event, Arlington, Virginia (Apr. 30, 2019).

[6] Al Amine, Majed, Kenneth Mathias, and Thomas Dyer. "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities." ACCENTURE STRATEGY, 2017 at p.11, available at: https://newsroom.accenture.com/content/1101/files/Accenture_5G-Municipalities-Become-Smart-Cities.pdf (last visited Sept. 30, 2019).

[7] *See, e.g.*, Aron Report at para. 150 (citing Jerry Hausman, "Valuing the Effects if Regulation on New Services in Telecommunications," Brookings Papers: Microeconomics (1997)).

stimulating carrier expenditures and generating the jobs necessary for rolling out 5G infrastructure.[8] Rapidly deploying 5G networks also would indirectly benefit the U.S. economy by facilitating the development and distribution of innovative goods and services within the 5G ecosystem.[9] This effect would accelerate as U.S. consumers grow increasingly dependent on devices that are part of the Internet of Things. Indeed, the delay in 5G deployment resulting from the unavailability of mid-band spectrum is already costing the U.S. economy.[10] Dr. Aron calculates that the further delay resulting from excluding Huawei from the U.S. market could result in *additional* losses to the U.S. economy from approximately $104 billion to $241 billion.[11]

Third, Dr. Aron discusses the effect that delayed 5G deployment will have on U.S. employment by directly reducing the number of available jobs in industries related to the rollout of 5G networks, including but not limited to manufacturing, construction, and engineering. Job losses in these "direct" industries will cause further reduced employment in industries that typically supply inputs to "direct" industries, such as support jobs at restaurants and grocery stores

---

[8] *See, e.g.*, Dan Littmann, Phil Wilson, Craig Wigginton, Brett Haan, and Jack Fritz. "5G: The Chance to Lead for a Decade," DELOITTE, 2018 at p.11, available at: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-5g-deployment-imperative.pdf (last visited Sept. 30, 2019).

[9] *See id.* at 9-11; *see also, e.g.*, "The 5G Era: Age of Boundless Connectivity and Intelligent Automation," GSMA, 2017, available at: https://www.gsmaintelligence.com/research/?file=0efdd9e7b6eb1c4ad9aa5d4c0c971e62&download (last visited Sept. 30, 2019); Steve Lo and Kevin Lee, "China is Poised to Win the 5G Race: Key Steps Extending Global Leadership," ERNST & YOUNG, 2018 at pp. 27-35, available at: https://www.ey.com/Publication/vwLUAssets/ey-china-is-poised-to-win-the-5g-race-en/$FILE/ey-china-is-poised-to-win-the-5g-race-en.pdf (last visited Sept. 30, 2019).

[10] *See* Aron Report at Section V.B, para. 79 ("The United States is therefore at a material disadvantage in competing for leadership in 5G deployment with countries in which mid-band spectrum has already been allocated (e.g., China, Japan, and South Korea), while in the United States mid-band spectrum is unavailable to three of the four top carriers and no clear timeline for its allocation has been established.").

[11] *See* Aron Report at para. 186.

that may cater to construction and related activities. Dr. Aron's quantitative analysis predicts that delayed 5G investment caused by Huawei's exclusion in the U.S. market would cause, at minimum, a loss of 25,200 jobs in 2019, and up to an additional 50,300 jobs lost in 2020.[12]

Finally, Dr. Aron analyzes how excluding Huawei from the United States market would reduce competition in the 5G equipment market and therefore impose increased costs on carriers and consumers. In turn, that reduced competition would further result in reduced deployment of 5G networks in less urban areas, where the potential economic returns on 5G infrastructure investment are less certain. Specifically, the U.S. market for RAN equipment is already overly concentrated, with an estimated Herfindahl–Hirschman Index ("HHI") concentration measure of between 2,964 and 3,125—and an HHI above 2,500 indicates a highly concentrated market. Yet excluding Huawei would elevate this number to 4,071. U.S. Department of Justice and Federal Trade Commission Guidelines predict that such a significant increase enhances existing participants' market power, causes prices to rise, and damages social welfare.[13] In fact, Dr. Aron estimates that Huawei's absence from the U.S. market will result in 12.6-16% higher weighted average prices for RAN equipment than if Huawei were not excluded.[14] Conversely, allowing Huawei to compete in the U.S. market would not only generate substantial downward pricing pressure on Huawei's competitors, but also encourage Huawei's competitors to develop more innovative products.[15] That additional competition and price reduction would help to close the

---

[12] *See* Aron Report at para. 194.

[13] *See* U.S. Dep't of Justice & Fed. Trade Comm'n, Horizontal Merger Guidelines § 5.3, at 18-19 (Aug. 19, 2010), available at https://www.justice.gov/sites/default/files/atr/legacy/2010/08/19/hmg-2010.pdf (last visited Sep. 30, 2019).

[14] *See* Aron Report at para. 213.

[15] *See id.* at para. 218.

broadband divide by encouraging carriers to deploy 5G equipment more broadly and quickly, particularly to the benefit of rural areas where challenging economies of scale make access to competitively priced equipment essential to the business and investments case to rollout 5G networks.

The Commission's proposed rule will have a disproportionately negative affect on rural economies and the lives of rural Americans. The Commission recognizes that the myriad benefits accompanying broadband access—such as employment and educational opportunities, innovations in health care and telemedicine, and connectivity among families and communities—can be "even more important in America's more remote small towns, rural, and insular areas."[16] This is particularly true with respect to 5G deployment, which has been widely regarded as a "digital revolution" capable of providing transformative technological solutions for Americans across the country.[17] Indeed, Commission leadership has repeatedly acknowledged the importance of 5G networks for rural Americans.[18] But many communities in rural America already fear that

---

[16] *Connect America Fund, ETC Annual Reports and Certifications, Establishing Just and Reasonable Rates for Local Exchange Carriers, and Developing a Unified Intercarrier Compensation Regime*, Report and Order, Third Order on Reconsideration, and Notice of Proposed Rulemaking, WC Docket No. 10-90 *et al*., (rel. Mar. 23, 2018) at para. 2.

[17] *See, e.g.*, Remarks of FCC Chairman Ajit Pai, National Spectrum Consortium 5G Collaboration Event, Arlington, Virginia (Apr. 30, 2019) (highlighting that "5G will power smart transportation networks that reduce traffic, prevent accidents, and limit pollution. 5G will enable healthcare professionals to remotely monitor your health and transmit data to your doctor before problems become emergencies. 5G will empower farms to apply precision agriculture. And, of course, 5G will unlock innovations that are yet to be imagined.").

[18] *See, e.g.*, Remarks of FCC Chairman Ajit Pai at the White House, Washington, D.C. (Apr. 12, 2019) ("The second reason U.S. leadership matters is that 5G will improve Americans' lives in so many ways. From precision agriculture to smart transportation networks to telemedicine and more, we want Americans to be the first to benefit from this new digital revolution, while protecting our innovators and citizens. And we don't want rural Americans to be left behind."); Remarks of FCC Commissioner Brendan Carr, "Grassroots Leadership on 5G", Indianapolis, Indiana (Sep. 4, 2018) at 2 ("When I think about success—when I think about winning the race to 5G—the finish line is not the moment we see next-gen

"they may be left behind" when it comes to 5G deployment.[19] The proposed rule will only serve to widen the digital divide in rural areas. Rural carriers providing services to remote or underserved areas of the United States, where adequate communications services are already scarce, depend especially on USF support due to challenging economies of scale in areas that lack dense populations.[20] As the record demonstrates, some rural carriers may be entirely unable to sustain operations under the proposed rule.[21] Adopting policies that increase carriers' costs to deploy 5G networks will not only increase corresponding costs charged to rural consumers, but will result in disproportionate delays to rural communities in the deployment of 5G network infrastructure itself. This, in turn, will slow the "virtuous cycle" where deploying broadband networks spurs new uses and applications of such technology, fostering increased demand for such networks, leading to increased investment in such networks, and refreshing the cycle.[22]

---

deployments in New York or San Francisco. Success can only be measured when all Americans, no matter where they live, have a fair shot at fast, affordable broadband.").

[19] Remarks of FCC Commissioner Brendan Carr, "Grassroots Leadership on 5G", Indianapolis, Indiana (Sep. 4, 2018).

[20] *See Multi-Association Group Plan for Regulation of Interstate Services of Non-Price Cap Incumbent Local Exchange Carriers and Interexchange Carriers et al.*, Second Report and Order and Further Notice of Proposed Rulemaking, Fifteenth Report and Order and Report and Order, CC Docket No. 96-45 *et. al*, 16 FCC Rcd 19613, 19617, para. 4 (2001) (recognizing that smaller carriers "generally have higher operating and equipment costs ... due to lower subscriber density, smaller exchanges, and limited economies of scale").

[21] *See, e.g.*, Comments of the Rural Broadband Alliance, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89 (June 1, 2018), at 14 (labeling the proposed rule as "an existential threat to the entire business"); Comments of the Mark Twain Telephone Company, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89 (June 1, 2018), at 3-4 ("the costs associated with the replacement of existing equipment … impos[e] a significant and unreasonable financial burden on rural telecommunications companies").

[22] *See, e.g.*, Remarks of FCC Chairman Ajit Pai, Mobile World Congress Americas, San Francisco, California (Sept. 12, 2017) (discussing the need to "close the digital divide and boost network investment" with "an eye toward revving the virtuous cycle of faster, better networks that unleash new innovations that drive additional consumer demand").

Huawei urges the Commission to consider carefully the substantial harms its proposed rules would inflict on U.S. carriers, consumers, and the economy; and whether there are less costly and more effective means available to achieve its network security goals. Huawei stands ready to work with the Commission to develop a vendor-independent, supply-chain cybersecurity process like that recommended by the National Institute of Standards and Technology.[23] As Huawei has previously noted, a number of U.S. Government officials support a vendor-agnostic approach to supply chain security, and many U.S. allies, including Germany, France, the United Kingdom, and Canada, have also expressed a desire for a holistic approach to managing risk in the telecommunications supply chain.[24]

Huawei recognizes the importance of creating secure telecommunications networks. But the Commission's proposed rule does not do so. Instead, it only serves to exacerbate the widening gap in 5G deployment between the United States and other countries. Dr. Aron demonstrates that delayed 5G deployment will impair the U.S. economy by depressing competition and reducing available jobs to U.S. workers. Moreover, these harms will be felt greatest by Americans in rural and undeserved areas. The Commission should support a comprehensive, holistic approach to supply-chain security based on existing best practices instead of focusing on proscriptions based on vendor's country of origin that would do little to advance supply-chain security. Moreover, as

---

[23] *See* National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Ver 1.1 (Apr. 16, 2018) available at https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited Sept. 30, 2019); National Institute for Standards and Technology, Supply Chain Risk Management for Federal Information Systems and Organizations, NIST Special Publication 800-161 (2015) available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf (last visited Sept. 30, 2019).

[24] *See* Written Ex Parte Submission of Huawei Technologies Co., Ltd and Huawei Technologies USA, Inc., *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89 (Jul. 12, 2019) at pp. 5-8.

the Commission considers adopting rules and policies to ensure the integrity of U.S. communications networks, it must do so in a targeted manner consistent with established best practices in order to avoid delaying 5G deployment, hindering competition and negatively impacting employment in the United States.

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, D.C. 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.

October 11, 2019

Exhibit 15-A

Expert Report of Dr. Debra J. Aron

The Impact on the U.S. Economy of Excluding Huawei from Participation in the U.S. Market for Wireless Network Equipment

EXPERT REPORT

of

Dr. Debra J. Aron
Charles River Associates
October 7, 2019

Table of Contents

I. QUALIFICATIONS 1

II. SUMMARY OF CONCLUSIONS 3

III. PURPOSE OF THIS REPORT 6

IV. BACKGROUND 8
- A. The Evolution of Wireless Telecommunications Technology 8
- B. 5G Technology Will Enable Transformative Benefits and Uses 18

V. THE SPECTRUM "GAP" IN THE UNITED STATES 22
- A. U.S. Policy Regarding 5G Deployment 22
- B. The State of 5G Deployment in the United States and the Rest of the World 23
  - i. Key Spectrum Bands Are Currently Unavailable to Carriers in the United States 23
  - ii. The United States Is Currently Well Behind Other Countries in 5G Deployments 28

VI. THE MARKET FOR RAN NETWORK EQUIPMENT IN THE UNITED STATES AND THE REST OF THE WORLD 30

VII. HUAWEI HAS UNIQUE CHARACTERISTICS WHOSE CONTINUED ABSENCE WILL DELAY THE U.S. TRANSITION TO 5G 38
- A. Huawei Is an R&D Leader in 5G 38
- B. Huawei's 5G RAN Equipment Is More Highly Ranked Than 5G RAN Equipment of Its Competitors 44
- C. Huawei's Massive MIMO Equipment Is in Far Greater Demand Than That Available from Any Other Vendor 45

VIII. CONTINUING TO LIMIT HUAWEI'S PARTICIPATION IN THE U.S. MARKET WILL DELAY THE U.S. TRANSITION TO 5G 51
- A. Early Deployment of New Wireless Technology Benefits a Country 51
- B. Impacts of Wireless Telecommunications Technology on Economic Growth and Productivity 52
- C. Continued Exclusion of Huawei Will Further Delay 5G Deployment and Penetration 55
  - i. Huawei's RAN Equipment, Especially Massive MIMO, Is Among the Most Widely Used in the World, Thus Implying a More Developed Ecosystem that Facilitates Deployment and Adoption 57
  - ii. Huawei's Competitive Presence Would Drive Down Prices of Other Vendors' RAN Equipment, Thus Encouraging Faster Deployment of 5G 57
  - iii. Simultaneous Deployment of 5G Around the World Imposes Pressure on the Global Supply Chain of RAN Equipment, Leading to Delays 58
  - iv. Huawei's 5G RAN Equipment Is the Most Advanced in the World, and Its Absence Will Affect the Quality of Services Available to U.S. Mobile Wireless Customers, Thereby Depressing Customer Acceptance 58
- D. Other Observers Have Also Concluded that Exclusion of Huawei Will Cause Delay in 5G Network Deployment 59

E. The Economic Impact of the Delay of 5G Deployment on the U.S. Economy, Incorporating the Effects of Depressed Penetration 60
i. Estimating the Effect of 5G Penetration on GDP 61
ii. Modeling the Delay Due to the Absence of Huawei 62
iii. Calculation of the Effect of Delayed 5G Deployment on the U.S. Economy Due to Exclusion of Huawei.....64
iv. Calculation of the Effect of Delayed 5G Deployment on U.S. Employment Due to Exclusion of Huawei.....69

IX. THE IMPACT ON THE COSTS OF RAN EQUIPMENT DUE TO REDUCED COMPETITION FROM EXCLUDING HUAWEI FROM THE U.S. MARKET FOR RAN NETWORK EQUIPMENT 77

I. QUALIFICATIONS

1. My name is Debra J. Aron. I am a Vice President at Charles River Associates ("CRA"). CRA is an international consulting and expert services firm that provides, among other services, economic expertise for litigation, regulatory proceedings, policy debates, and business strategies.

2. I received a Ph.D. in economics from the University of Chicago in 1985, where my honors included a Milton Friedman Fund fellowship, a Pew Foundation teaching fellowship, and a Center for the Study of the Economy and the State dissertation fellowship.

3. From 1985 to 1992, I was an Assistant Professor of Managerial Economics and Decision Sciences at the J. L. Kellogg Graduate School of Management, Northwestern University. Concurrent with my position at Northwestern University, I also held the position of Faculty Research Fellow with the National Bureau of Economic Research from 1987 to 1990.

4. I was named a National Fellow of the Hoover Institution, a think tank at Stanford University, for the academic year 1992-1993, where I studied innovation and product proliferation in multiproduct firms. From 1993 to 1995, I was a Visiting Assistant Professor of Managerial Economics and Decision Sciences at the Kellogg School. At the Kellogg School, I taught M.B.A. and Ph.D. courses in managerial economics, information economics, the economics and strategy of pricing, and the economics of competitive strategy.

5. I continued to teach economics and business strategy as an Adjunct Associate Professor in the Masters of Science in Communications program at Northwestern University in most years between 2000 and 2016. In that program I taught a graduate course in economics and competitive strategy with a focus on communications markets.

6. I am a member of the American Economic Association and the Econometric Society and an associate member of the American Bar Association. I have published scholarly articles on innovation, competition, incentives, and pricing in several leading academic journals, including the American Economic Review, the RAND Journal of Economics, and the

Journal of Law, Economics, and Organization. I am co-author of the economics chapter of the American Bar Association's Section of Antitrust Law Telecom Antitrust Handbook.

7. Much of my consulting and scholarly work in the last twenty years has pertained to the telecommunications industry. My work has included economic analysis for litigation, regulatory disputes, public policy, merger analyses, and business consulting. Areas of analysis have involved wireless telephony, wireline telecommunications, broadband, and satellite communications and retail, wholesale, and equipment markets. I have written, testified, and published scholarly work on matters related to the demand for and the costs of advanced telecommunications services. I am familiar with and have examined the costs, revenues, networks, subscribers, usage, and other data of telecommunications companies. Telecommunications and technology matters in which I have testified have included class actions, contract disputes, antitrust litigation, mergers, regulatory proceedings, arbitrations, and intellectual property matters. My clients have included numerous telecommunications companies in the United States and abroad, including both large and small wireless telecommunications companies and telecommunications equipment companies.

8. I have submitted evidence to the U.S. Federal Communications Commission ("FCC") regarding, among other topics, the measurement of competition and market power in telecommunications markets and telecommunications pricing and costing standards. My scholarly work has been cited by the FCC. I have also testified in a number of states on regulatory issues pertaining to broadband markets, broadband deployment, and incentives for broadband investment.

9. My professional qualifications are further detailed in my curriculum vitae, which is attached as Exhibit I.1 to this report.

10. I have prepared this report at the request of Huawei Technologies Co., Ltd, and have been compensated by Huawei for my work. This report represents my independent assessment and opinions.

II. SUMMARY OF CONCLUSIONS

11. The development and production of wireless infrastructure equipment is a highly technical and research-intensive business, yet it is critical to the ability of wireless telecommunications carriers to deploy new, ground-breaking technologies. There are only five companies worldwide that have demonstrated the expertise and capabilities to be in that business, and only three have significant shares of global sales. Even among that limited group, Huawei Technologies Co., Ltd. ("Huawei") is the leader in equipment sales, research and development ("R&D") spending, product performance, patent production for the newest technology, and several other metrics that demonstrate its worldwide leadership role as a premier provider of the equipment required to deploy advanced and innovative wireless networks.[1]

12. The exclusion of Huawei from the opportunity to compete in the U.S. market has harmed the U.S. economy and will, if continued, substantially impede the ability of the United States to achieve its goal of leadership in the deployment of the newest network technology now being rolled out worldwide, known as "5G." 5G technology is expected to not only provide massive capacity, speed, and latency improvements over existing wireless technology, but to transform many existing industries and create new ones. 5G technology is anticipated to enable innovation in transportation, logistics, the Internet of Things ("IoT"), electricity distribution, public safety, and health and wellness, among others.

13. Economic studies have found that adoption of new wireless technologies translates into real economic benefits for a country. Several studies find that the global leaders in previous generations of wireless networks were awarded greater macroeconomic benefits, including job creation and increased gross domestic product ("GDP"), than non-leading countries. These benefits arise through the development of a wireless ecosystem of new products and services that support and are supported by the new technology.

[1] I understand that among the Huawei entities, Huawei Technologies Co., Ltd., a wholly owned subsidiary of the Huawei Investment & Holding Co., Ltd., is the entity primarily responsible for "development, manufacture and sale of telecommunication and related products and provision of support and maintenance services." See Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 123.

14. Huawei has developed differentiated expertise relative to other vendors of 5G equipment. One of the key technologies deployed in 5G networks is Massive MIMO, which is a multiple input, multiple output active antenna system. Massive MIMO is based on a technology in which, for historical reasons, Huawei had developed exceptionally extensive expertise and experience. Perhaps as a result, Huawei has by far the largest revenue share in the market for Massive MIMO. The evidence indicates, and multiple industry participants have concluded, that Huawei has the most advanced Massive MIMO products available in the market today.

15. Huawei is also considered a leader in 5G radio access network ("RAN") equipment overall based on (1) baseband unit ("BBU") capacity, (2) breadth of its radio unit ("RU") portfolio, (3) ease of installation, and (4) ease of upgrade from 4G to 5G. A recent report by market research firm GlobalData found Huawei's 5G RAN equipment to lead in every category considered.[2]

16. The United States is already behind other leading countries in the "race" to 5G, as measured by early expenditures on 5G equipment. Access to the most advanced and most accepted equipment available is particularly important in the United States because of what is sometimes referred to as the U.S. spectrum "gap." Spectrum bands in the mid-frequencies ("mid-band spectrum") are necessary for economical nationwide broad-based deployment of 5G. In the United States, however, significant mid-band spectrum has not yet been made available for mobile use, and three of the four major U.S. wireless carriers currently lack access to any portion of mid-band spectrum. Most of the countries around the world already planning, testing, or deploying 5G networks are using mid-band spectrum.[3]

17. U.S. carriers, in contrast, are conducting initial deployments largely in other spectrum bands that may be appropriate for certain uses (primarily, either fixed wireless broadband replacement, or very high-density locations) but not for large scale mobile deployment.

18. The spectrum gap has already delayed 5G deployment and adoption in the United States compared to other leading countries that have successfully deployed and launched 5G

[2] See Section VII.B.
[3] See Section V and Appendix D.

networks. The absence of Huawei—a technology leader in 5G RAN in general and in Massive MIMO in particular—from the U.S. market for 5G RAN equipment will inevitably damage the United States' ability to regain lost ground to the extent it is possible once mid-band spectrum is finally allocated, and cause additional delays in 5G deployment and adoption.

19. In addition, exclusion of Huawei from the U.S. market is likely to work to the detriment of 5G service quality in the United States relative to that in other countries. History has shown that despite its early adoption of 4G technology, the United States—in which Huawei has never had a material sales share—has far slower networks than dozens of countries in Europe, Asia, and the rest of the world, all regions where Huawei is the largest equipment vendor.

20. I have estimated the effect on the U.S. economy of a delay in 5G deployment and adoption that would be associated with continued absence of Huawei from the U.S. market. I estimate that the present discounted value of losses to U.S. GDP would vary from approximately $104 billion (for a 6-month delay) to approximately $241 billion (from an 18-month delay), over and above the effects on the U.S. economy associated with the delay in 5G deployment caused by the spectrum gap in the United States. In addition, I estimate that delayed infrastructure investment due to the absence of Huawei would depress employment by 25.2 thousand jobs in 2019 and by up to 50.3 thousand jobs in 2020, depending on the duration of delay.

21. The absence of Huawei from the U.S. market would also be expected to weaken competition in a highly concentrated marketplace in which, by the most recent statistics, almost 90 percent of sales of radio access network equipment was provided by only two companies, Nokia and Ericsson. I estimate that the absence of Huawei in the U.S. market for RAN equipment has materially increased market concentration, resulting in prices for RAN equipment that are 12.6-16.0 percent higher on a weighted average basis than they would be with the competition provided by Huawei. An increase in prices of 12.6-16.0

percent is considered material and harmful to social welfare.[4] I would expect some, if not all, of this increase in carriers' costs of building and upgrading their networks to be passed through in the form of higher prices for wireless services paid by consumers, businesses, and the government. Further, it will likely prompt wireless carriers to deploy less 5G infrastructure in rural and other areas where the business case for deployment may be marginal.

22. This analysis does not include the cost to consumers, businesses, and government customers of depressed incentives of other vendors to intensify their R&D efforts and of inferior network performance that would be expected from excluding from the market for 5G RAN equipment the vendor that is demonstrably the most technologically accomplished.

III. PURPOSE OF THIS REPORT

23. I understand that in 2018, the FCC initiated this proceeding to consider whether to adopt a rule that would have the effect of prohibiting the use of universal service funds for the purchase of equipment or services from providers identified as posing a national security risk.[5] The FCC specifically identified Huawei as a company that it evidently considers a candidate to be designated as a supplier to which that prohibition would apply.[6]

24. Huawei's presence in the U.S. market for RAN equipment has been very limited for several years, reportedly as a result of several policy and political interventions.[7] Continuing to limit Huawei's presence in the United States and imposing additional restrictions would prevent Huawei from becoming a competitor and supplier on a level playing field with the other major global providers of RAN equipment who supply carriers in the United States. Indeed, I understand most of Huawei's business as a telecommunications equipment

[4] See Section IX.

[5] See Notice of Proposed Rulemaking, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Before the Federal Communications Commission, WC Docket No. 18-89, FCC 18-42 (Released: April 18, 2018), ¶ 2.

[6] See Notice of Proposed Rulemaking, *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Before the Federal Communications Commission, WC Docket No. 18-89, FCC 18-42 (Released: April 18, 2018), ¶¶ 4-6.

[7] See Section VI for a more detailed discussion of these political and policy interventions.

supplier in the United States is to universal service fund recipients and, thus, barring use of such funds for purchase of Huawei equipment might well have the practical effect of excluding Huawei from the U.S. market.

25. I have been asked by Huawei to assess the economic effects on the U.S. marketplace and economy of excluding Huawei from selling its products and services in the United States. In this report I quantify the effects on the price of telecommunications network equipment, GDP, and employment of excluding Huawei from the opportunity to provide RAN telecommunications equipment in the United States. All analyses conducted and opinions expressed in this report are my own, independent of the interests or opinions of Huawei or any other entity. The data used in this report to support my opinions are also independent, third-party data not provided by Huawei.

26. Excluding Huawei from the United States has already had and will continue to have significant economic effects. I analyze two significant avenues of economic effects in this report. One avenue of economic impact from banning Huawei from the U.S. marketplace is that excluding any of the major global vendors of wireless network equipment will dampen competition that benefits U.S. wireless services suppliers and consumers. Equipment vendors compete to provide wireless carriers with the best combination of price, quality, and product features. As I will discuss, there are only a few companies that offer RAN infrastructure equipment, and even fewer that make large, ongoing investments in R&D for that equipment. Excluding one of those market participants from competition dampens competition in the provision of network equipment in the United States and results in higher equipment prices paid by U.S. wireless carriers.

27. But perhaps even more importantly and more urgently, continuing to exclude Huawei from the United States is particularly damaging because the United States—and the world—are at the inception of a transition to the next and most advanced wireless technology. Known as 5G ("fifth generation"), this technology is expected to transform the way we live and work. Because certain spectrum bands critical for 5G deployment are currently not available to three out of four major U.S. carriers, the deployment of 5G networks has already been delayed in the United States, and the United States is already behind other

countries in 5G network investment. Excluding Huawei from the United States is likely to further delay the United States' deployment and adoption of 5G, with ripple effects throughout the economy. These effects are the primary focus of my report.

28. This report concentrates on the components of wireless networks known as the Radio Access Network, or "RAN." A wireless network generally consists of the RAN, the core network, and other components providing transport between the RAN and the core. The RAN is responsible for the radio-related functionality of the network, including transmitting signals between the users' handsets and the core network, while the core network's main functionality is to manage and route voice and data traffic between the RAN and other data networks, such as the internet. RAN equipment includes antenna systems and base stations that transmit and receive the signals. Core equipment includes routers and switches.[8] I focus on the 5G RAN components because the 5G RAN is generally being deployed first in order to enable and operationalize a new generation of technology, while relying on the existing core and upgrading it later.[9] Accordingly, the economic impact of the delay caused by the inability to use Huawei equipment in the United States would be experienced first with respect to its RAN equipment.

29. This report does not offer any opinion on national security aspects, if any, of Huawei's telecommunications network equipment.

IV. BACKGROUND

A. The Evolution of Wireless Telecommunications Technology

30. The rapid and transformative developments of wireless communications technologies over the last four decades have been categorized into five "generations."

[8] See REGULATION (EC) NO 139/2004 MERGER PROCEDURE: ARTICLE 6(1)(B) NON-OPPOSITION, "Case No COMP/M.7632 – NOKIA/ALCATEL-LUCENT," July 24, 2015 (hereafter, *Nokia/Alcatel-Lucent Merger Procedure 2015*), pp. 2, 3, 8-9.

[9] Irina Cotanis, "5 Critical 5G Network Deployment Challenges," Infovista Blog, August 15, 2019, at https://www.infovista.com/blog/5g-network-deployment-challenges?utm_source=facebook&utm_medium=update.

31. The first country to launch a first generation ("1G") commercial network was Japan in 1979. 1G was an analog system and offered no data capabilities—that is, it was a voice-only communications system.[10] Despite its limited capabilities and capacity, 1G analog wireless technology ushered in a new era in which telephony was not confined to a wireline phone, allowing voice communications to go mobile.

32. The limitations of analog wireless telephony soon became apparent. Analog systems make very inefficient use of spectrum, so that a given amount of spectrum could support a relatively small volume of telephone calls[11] and calls were therefore very expensive.[12] In response to the economic and technical limitations of 1G technology, the second generation ("2G") of wireless technology emerged in the late 1980s and was the first digital wireless technology.[13] Digital technology not only allowed much more efficient use of spectrum, thereby supporting much higher call volumes and reducing the cost of service, but it also enabled certain basic data services, such as texting.[14]

33. There were several versions of 2G technology that used different technology standards.[15] Two of the major 2G standards worldwide were Global System for Mobile Communications ("GSM") and IS95 Code Division Multiple Access ("CDMA").[16] Europe coordinated on a single standard—GSM—which was endorsed by the European Council

---

[10] Prasant Kumar Pattnaik and Rajib Mall, FUNDAMENTALS OF MOBILE COMPUTING (PHI Learning Pvt. Ltd., 2015), p. 32. See also, Lopa J. Vora, "Evolution of Mobile Generation Technology: 1G to 5G and Review of Upcoming Wireless Technology 5G," *International Journal of Modern Trends in Engineering and Research* 2, iss. 10 (October 2015) (hereafter, *Vora 2015*), p. 281.

[11] *Vora 2015*, pp. 281-282.

[12] Prasant Kumar Pattnaik and Rajib Mall, FUNDAMENTALS OF MOBILE COMPUTING (PHI Learning Pvt. Ltd., 2015), p. 34.

[13] The first 2G network was launched in Finland in 1991. Ilya Grigorik, HIGH PERFORMANCE BROWSER NETWORKING (O'Reilly Media, Inc., 2013) (hereafter, *Grigorik 2013*), at https://hpbn.co/mobile-networks; and *Vora 2015*, p. 282.

[14] *Vora 2015*, p. 282; Jeffrey L. Funk and David T. Methe, "Market- and committee-based mechanisms in the creation and diffusion of global industry standards: the case of mobile communication," *Research Policy* 30, no. 4 (2001) (hereafter, *Funk and Methe 2001*), p. 593.

[15] *Grigorik 2013*. Technology standardization is the process of creating systems, products, and services within a set of guidelines. Developing a new telecommunications technology standard involves a number of parties, including telecommunications equipment vendors, carriers, users, interest groups, and governments. Standardization helps to ensure systems' interoperability, safety, quality, and repeatability. "Setting the standard," Ericsson, at https://www.ericsson.com/en/future-technologies/standardization.

[16] *Funk and Methe 2001*, pp. 600-601. For the definition of GSM, see *Grigorik 2013*.

and which was adopted by most European carriers.[17] The United States, however, took a more laissez-faire approach and, rather than orchestrating the adoption of one standard, left each carrier to select the standard it preferred.[18]

34. AT&T Wireless adopted a standard known as Time Division Multiple Access ("TDMA"), which was closely related to GSM.[19] T-Mobile (formerly VoiceStream Wireless) adopted the GSM standard.[20] Sprint and Verizon Wireless, however, were among the relatively few major carriers in the world to adopt CDMA.[21]

35. Researchers have argued that Europe's coordination on a single telecommunications standard facilitated deployment by reducing carriers' uncertainty in committing to the GSM standard and allowing European countries to launch 2G networks ahead of other countries.[22] In the United States, the lack of coordination on a single standard is thought to have created uncertainty among U.S. carriers over which standard to adopt, retarding the widespread adoption of 2G networks in the United States.[23]

36. There are several factors that determine successful dissemination of a new technology standard such as GSM or CDMA. One is whether a large number of carriers adopt it. When many carriers adopt a technology, equipment vendors (which include network equipment suppliers and handset suppliers) have a greater incentive to manufacture standard-specific equipment. The more vendors that produce equipment for that standard,

---

[17] *Funk and Methe 2001*, p. 600; Rudi Bekkers, Geert Duysters, and Bart Verspagen, "Intellectual property rights, strategic technology agreements and market structure: The case of GSM," *Research Policy* 31 (2002) (hereafter, *Bekkers et al. 2002*), p. 1145, fn. 5.

[18] *Funk and Methe 2001*, pp. 600-601.

[19] Jerry Hausman, "Mobile Telephone," in HANDBOOK OF TELECOMMUNICATIONS ECONOMICS, VOLUME 1: STRUCTURE, REGULATION AND COMPETITION, eds. Martin E. Cave, Sumit K. Majumdar, and Ingo Vogelsang (Amsterdam: Elsevier Science B.V, 2002) (hereafter, *2002 Hausman*), p. 568. For the definition of TDMA, see *Funk and Methe 2001*, p. 601.

[20] Seventh Report, *In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993; Annual Report and Analysis of Competitive Market Conditions With Respect to Commercial Mobile Services*, Before the Federal Communications Commission, FCC 02-179 (Released: July 3, 2002) (hereafter, *7th CMRS Report*), fn. 61 and Section II.A.1.c.i.

[21] *2002 Hausman*, pp. 568-570.

[22] "How America's 4G Leadership Propelled the U.S. Economy," Recon Analytics, April 16, 2018 (hereafter, *Recon Analytics Report 2018*), p. 3; *Funk and Methe 2001*, pp. 600, 603-604.

[23] *Funk and Methe 2001*, pp. 600-601; *Recon Analytics Report 2018*, p. 3.

the more competition there is, which in turn results in lower equipment prices.[24] The greater the availability of equipment and handsets and the lower the prices, the more attractive the standard is to carriers who have not yet adopted a standard.[25] This creates a virtuous cycle that reinforces the success of the standard.

37. The industries that arise from the development of new wireless technologies, including handsets, applications, advertising, and other businesses that leverage the unique capabilities of wireless technologies, are collectively referred to as the wireless ecosystem.[26] Each development of a new generation of technology triggers economic development directly by growing the revenue opportunities of the wireless services providers, but also indirectly by encouraging innovation in other sectors of economy.

38. The United States was indeed very slow to develop 2G networks relative to the rest of the world. For example, in December 1994, Germany's 2G penetration rate (the percentage of the population that subscribed to 2G technology) was 71 percent, while the United States' 2G penetration rate was only 0.1 percent. The United States did not reach even 50 percent 2G penetration until 1999, at which point Japan, France, Germany, Italy, Spain, and the United Kingdom all had 2G penetration rates of over 90 percent, and most were close to 100 percent.[27] The United States did not catch up to the 2G penetration in other countries until nearly a decade after it began deploying 2G, at which point the other countries' 2G penetration rates were largely in decline as they had begun to deploy the third generation of mobile communications, "3G."[28]

---

[24] For example, when many carriers committed to GSM standard, this relieved suppliers' uncertainty about the potential market size for this standard and provided suppliers incentives to produce equipment for GSM. *Bekkers et al. 2002*, pp. 1145-1146.

[25] *Funk and Methe 2001*, p. 603.

[26] *2019 Global Race to 5G Analysys Mason Report*, p. 4, fn. 2.

[27] *Recon Analytics Report 2018*, pp. 3-4 and Exhibit 1.

[28] *Recon Analytics Report 2018*, pp. 3-4 and Exhibit 1.

39. 3G technology emerged around 2001 in Japan[29] and was the first true step to high-quality mobile broadband.[30] There were, again, two main competing 3G standards, which were the separate evolution paths of GSM and CDMA. Universal Mobile Telecommunication System ("UMTS"), also referred to as wideband CDMA ("WCDMA"),[31] was developed based on the GSM standard, and CDMA2000 was developed based on the CDMA standard.[32] A third 3G standard, Time Division-Synchronous Code Division Multiple Access ("TD-SCDMA"), which used Time Division Duplex technology, was developed and used in China.[33] High-Speed Download/Upload Packet Access ("HSPA") was an evolution of the UMTS 3G standard introduced in the early 2000s.[34]

40. Once again, the United States was very late to adopt the new technology relative to the rest of the world and especially relative to the 3G leader, Japan. In 2007, U.S. penetration of 3G was less than 10 percent, at which point Japan already had over 50 percent 3G penetration.[35]

41. To address the ever-increasing demand for higher data transmission speeds and lower latencies,[36] the 3rd Generation Partnership Project ("3GPP"), an organization responsible for the development of 3G and subsequent technologies,[37] redesigned the core and radio network technologies.[38] That effort led to the creation of the fourth generation ("4G") of

---

[29] Prasant Kumar Pattnaik and Rajib Mall, FUNDAMENTALS OF MOBILE COMPUTING (PHI Learning Pvt. Ltd., 2015), p. 36.

[30] Erik Dahlman, Stefan Parkvall, Johan Sköld, 5G NR: THE NEXT GENERATION WIRELESS ACCESS TECHNOLOGY (Academic Press, 2018) (hereafter, *Dahlman et al. 2018*), p. 1.

[31] "What is 3G UMTS: WCDMA Tutorial," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/3g-umts/what-is-umts-wcdma-tutorial.php.

[32] *Grigorik 2013*.

[33] "What is 3G TD-SCDMA," Electronics Notes, at https://www.electronics-notes.com/articles/connectivity/3g-umts/td-scdma.php.

[34] *Grigorik 2013*.

[35] Recon Analytics Report 2018, Exhibit 2.

[36] Low latency is important for real-time application and "streaming" applications such as video, for example. I provide a definition of latency in Section IV.B.

[37] *Grigorik 2013*.

[38] Radio access and core networks are fundamental parts of telecommunications networks. I define them later in this section.

mobile communications networks in 2008. 4G was deployed in large part through the Long Term Evolution ("LTE") standard.[39]

42. Unlike the previous generations of digital wireless technology, LTE was not bifurcated into a GSM evolution path and a CDMA evolution path. Rather, LTE was on the evolution path for both technologies.[40] All major carriers in the United States adopted LTE as their 4G technology.[41] LTE supports both time division duplex ("TDD") and frequency division duplex ("FDD") schemes.[42] I explain the difference between TDD and FDD, and their relevance to the current 5G transition, in Section VII.C. Most LTE networks adopted in the United States and globally have been using FDD technology.[43] The 3G TD-SCDMA standard developed and adopted by China evolved into LTE-TDD.[44]

43. Each generational improvement in wireless technology engendered a revolution in applications and services that developed in response to the new capabilities created. For example, 2G technology introduced texting, which has become more ubiquitous than voice calls in the United States[45] and enabled basic data services.

44. 3G technology supported much higher data transmission rates than 2G technology. 3G ushered in the era of social media on wireless devices, such as Facebook and dating apps.[46] 3G also triggered the development of wireless applications such as location-based services,

---

[39] *Grigorik 2013*.

[40] *Grigorik 2013*.

[41] For a period of time, Sprint attempted to develop and deploy another 4G technology called WiMAX, but this technology ultimately did not succeed, and Sprint pivoted to LTE. Brad Reed, "LTE vs. WiMAX," November 2, 2011, Network World, at https://www.networkworld.com/article/2182390/lte-vs--wimax.html.

[42] "LTE FDD, TDD, TD-LTE Duplex Schemes," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/4g-lte-long-term-evolution/tdd-fdd-td-lte-duplex-schemes.php.

[43] "LTE FDD, TDD, TD-LTE Duplex Schemes," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/4g-lte-long-term-evolution/tdd-fdd-td-lte-duplex-schemes.php; "GSA confirms 521 LTE networks launched, LTE-Advanced now mainstream," Global mobile Supplier Association, August 12, 2016, at https://gsacom.com/press-release/gsa-confirms-521-lte-networks-launched-lte-advanced-now-mainstream/.

[44] "What is 3G TD-SCDMA," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/3g-umts/td-scdma.php.

[45] "Corilyn Shropshire, "Americans prefer texting to talking, report says," *Chicago Tribune*, March 26, 2015, at https://www.chicagotribune.com/business/ct-americans-texting-00327-biz-20150326-story.html.

[46] Facebook's mobile site was launched in 2007, and its app was launched in 2010. See Taylor Casti, "The Evolution of Facebook Mobile," *Mashable*, August 1, 2013, at https://mashable.com/2013/08/01/facebook-mobile-evolution/. The first online dating apps appeared around 2007. Isabel Thottam, "The history of online dating," *eHarmony*, at https://www.eharmony.com/history-of-online-dating/.

instant messaging, video telephony, multimedia gaming, and live-video buffering, among others.[47]

45. LTE drives the most advanced generally available networks in the United States today.[48] LTE was the first digital wireless technology for which the United States had a leadership position in deployment,[49] and the advent of LTE technology has transformed the U.S. economy and the lives of its citizens. Many of the developments of the 3G era—video conferencing, mobile gaming, and other mobile applications—became viable because of the improved speeds and lower latencies of LTE networks.[50] LTE has allowed consumers to quickly and easily use the internet on their mobile devices, so that many of our daily activities, from booking airline tickets to ordering dinner, are now performed through mobile apps.

46. LTE has also transformed the way we acquire and listen to music (and transformed the music industry as a result)[51] and vastly improved the experience of streaming video to our mobile devices, thus transforming the market for pay television and creating new business models for video content.[52] The ability to stream video reliably has transformed police work[53] and healthcare.[54] It also enabled the creation of entirely new industries that have changed the way we live, such as ride-sharing, home-sharing, shopping and payment by

---

[47] Prasant Kumar Pattnaik and Rajib Mall, FUNDAMENTALS OF MOBILE COMPUTING (PHI Learning Pvt. Ltd., 2015), p. 36.

[48] "LTE Achieves 4 Billion Connections Worldwide at end of 2018 — 47% of all Cellular Connections," 5G Americas, March 20, 2019, at https://www.globenewswire.com/news-release/2019/03/20/1758189/0/en/LTE-Achieves-4-Billion-Connections-Worldwide-at-end-of-2018-47-of-all-Cellular-Connections.html.

[49] Recon Analytics Report 2018, pp. 6-7.

[50] Vora 2015, p. 283-284; *Grigorik 2013*.

[51] Zachary Evans, "How Social Media and Mobile Technology Has Changed Music Forever," August 24, 2015, Social Media Week, at https://socialmediaweek.org/blog/2015/08/social-mobile-changed-music/.

[52] Services that were not supported by the previous technology generations have become possible in 4G. These include high-definition mobile TV, video conferencing, and 3D television. See Prasant Kumar Pattnaik and Rajib Mall, FUNDAMENTALS OF MOBILE COMPUTING (PHI Learning Pvt. Ltd., 2015), p. 37.

[53] "Eyes on the Street: How Wireless Video Solutions Are Transforming Public Safety," Motorola White Paper, 2012, at https://www.naco.org/sites/default/files/documents/Video%20Solutions%20Transforms%20Public%20Safety.pdf.

[54] Daniel Newman, "Top Five Digital Transformation Trends in Heath Care," Forbes, May 7, 2017, at https://www.forbes.com/sites/danielnewman/2017/03/07/top-five-digital-transformation-trends-in-healthcare/#4184fa4b2561.

phone, and gaming on phones.[55] The ease of shopping and logistics have empowered companies such as Amazon to transform the retail economy and the way consumers purchase products from appliances to shampoo.[56]

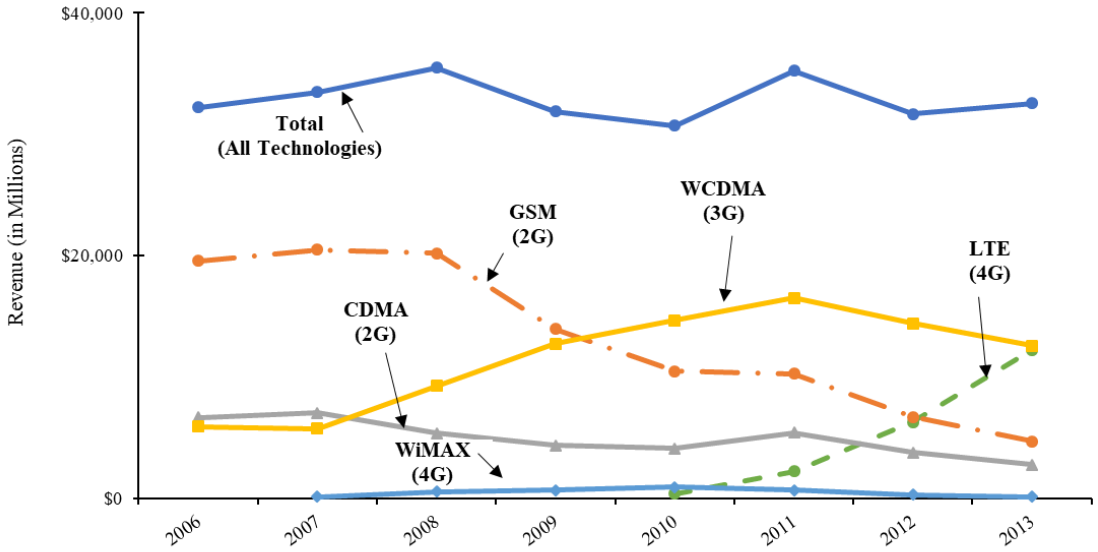
47. The timing of the rise and decline of each technology generation can be seen in the total worldwide RAN expenditures by carriers over time. Figure IV.1 shows the evolution of wireless RAN spending by technology from 2006 through 2013.[57] Since 2013, LTE RAN spending has significantly outpaced WCDMA spending and constituted the majority of RAN spending worldwide. 5G RAN sales started in Q4 2018 according to the data.

[55] Speaking at CTIA's 5G Summit, Sprint CEO Michel Combes claimed, "The U.S., and I know that from fact, was in Europe at that stage, was three years ahead of China and all the other countries in launching 4G. No one realized at that time, but it really gave U.S. businesses the opportunity to start an app revolution and now most of us can't imagine a world without apps like Uber, Facebook, and Instagram. Because of the high quality of American 4G networks and the hundreds of billions we invested, we have helped create the world's most valuable companies. In '16 alone, 4G contributed 100 billion dollars to the American economy, and it's fair to say that leadership in 4G to date has contributed more than a trillion dollars to the American economy." See, Michel Combes, Speech at CTIA's 5G Summit, April 4, 2019, at https://www.ctia.org/news/2019-5g-summit-event, at 07:29.

[56] Dennis Green, "Shopping changed a lot in 2017 – and smartphones are to blame," *Business Insider*, December 28, 2017, at https://www.businessinsider.com/mobile-shopping-exploded-this-year-2017-12.

[57] The data underlying Figure VI.1 were purchased under license from data vendor Dell'Oro Group. Here, and throughout this report, figures and analyses that rely on data from Dell'Oro Group have been purged of specific numbers and/or certain time periods per requirements of the data vendor.

Figure IV.1
Global Wireless Spending on Wireless RAN Equipment by Technology (in Millions), 2006-2013



Note: WiMAX data were not collected by Dell'Oro Group after 2015, because the revenues from WiMAX RAN equipment were very low.

Source: "TOTAL GSM," "TOTAL CDMA," "TOTAL WCDMA," "TOTAL LTE," "TOTAL 5G NR," Dell'Oro Group, Q1 2019.

48. 5G mobile technology is currently under development by 3GPP.[58] 3GPP is defining 5G standards in two releases: Release 15 and Release 16.[59] The first stage of Release 15, finalized by 3GPP in December 2017, defined the non-standalone ("NSA") 5G configuration, in which only the standards for 5G RAN, also known as 5G New Radio ("5G NR"),[60] were defined.[61] The second stage of Release 15 was finalized by 3GPP in June 2018, and it defined the standalone ("SA") 5G configuration, meaning that both the

[58] "3GPP Release 15 Overview." IEEE Spectrum, at https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview.

[59] "3GPP Release 15 Overview." IEEE Spectrum, at https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview.

[60] See "5G NR New Radio," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/5g-nr-new-radio.php. When I refer to radio access network in this report, I refer to both hardware (i.e., sites, antennas, base stations, etc.) and software needed to operate the hardware.

[61] David Abecassis, Janette Stewart, Chris Nickerson, "Global Race to 5G – Update," Analysys Mason, April 2019 (hereafter, *2019 Global Race to 5G Analysys Mason Report*), p. 17.

5G RAN and core networks were defined.[62] In March 2020, 3GPP is scheduled to finalize Release 16, which would provide further standardization of the 5G technology and its applications.[63] 5G standards are still being developed. As with other wireless generations, there will be future releases defining evolving standards for 5G.[64]

49. The first 5G deployments in the United States are NSA 5G networks.[65] Because the NSA configuration focuses on augmenting the RAN equipment in the carriers' networks (as opposed to the core equipment), the availability and quality of 5G RAN equipment is of primary importance for the early deployment of 5G in the U.S.

50. The first commercial 5G networks that enabled Fixed Wireless Access ("FWA") for end-users (access to 5G services via "fixed" user equipment such as hotspots, as opposed to access via mobile handsets[66]) were launched in 2018 by carriers in the United States and South Korea.[67] In April 2019, carriers in the United States and South Korea were also the first to launch commercial services that enabled consumers to access 5G networks via mobile handsets.[68] In addition, analysts have identified 201 carriers in 83 countries that are actively investing in 5G by obtaining licenses to conduct trials, are conducting tests and trials, deploying networks, or some combination of these activities.[69]

51. Appendix D summarizes the rapidly changing status of 5G deployments and launches worldwide as of this writing. I will discuss in Section VI that, as of today, South Korea is

---

[62] "3GPP Release 15 Overview." *IEEE Spectrum*, at https://spectrum.ieee.org/telecom/wireless/3gpp-release-15-overview.

[63] "Release 16," *3GPP*, updated July 16, 2018, at https://www.3gpp.org/release-16.

[64] "Release 17," *3GPP*, at https://www.3gpp.org/release-17; "3GPP 3GPP Specification Release Numbers," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/3gpp/standards-releases.php.

[65] Irina Cotanis, "5 Critical 5G Network Deployment Challenges," Infovista Blog, August 15, 2019, at https://www.infovista.com/blog/5g-network-deployment-challenges?utm_source=facebook&utm_medium=update.

[66] "Fixed Wireless Access," Redline Communications, at https://rdlcom.com/fixed-wireless-access/.

[67] See Appendix D.

[68] See Appendix D.

[69] *2019 Global Race to 5G Analysys Mason Report*, p. 8.

well ahead of other countries, including the United States, in commercial deployment of 5G, reporting over one million subscribers.[70]

B. 5G Technology Will Enable Transformative Benefits and Uses

52. Just as the previous generational improvements in wireless technology instigated sea changes in the wireless ecosystem and in our lifestyles, 5G is likely to usher in new products, services, and ways of interacting with each other and the world that will change our lives and affect our economy.

53. 5G technology provides massive capacity, speed, and latency improvements over 4G. Given these technological improvements over 4G, there are four major applications currently anticipated for 5G.[71]

54. Latency refers to the delay between when a customer makes a request for data and when those data are returned.[72] Capacity is the amount of traffic that a network can handle at any given time, such as the number of simultaneous calls and maximum data speeds.[73]

55. First, because of its substantial capacity increases, 5G will alleviate some of the capacity constraints on existing 4G networks. The use of 5G for the enhancement of current mobile broadband services and applications is known as enhanced mobile broadband ("eMBB").[74]

---

[70] Jeremy Horwitz, "South Korea hits 1 million 5G subscribers in 69 days, beating 4G record," *Venture Beat*, June 12, 2019, at https://venturebeat.com/2019/06/12/south-korea-hits-1-million-5g-subscribers-in-69-days-beating-4g-record/.

[71] The set of objectives for the first three use cases—eMBB, massive machine type communications, and ultra-reliable and low latency communications—known as International Mobile Telecommunications for 2020 ("IMT-2020") were developed by the International Telecommunications Union ("ITU"), which is a specialized agency of the United Nations that focuses on the global allocation of spectrum. See "About International Telecommunications Union (ITU)," *ITU*, at https://www.itu.int/en/about/Pages/default.aspx; "IMT Vision—Framework and overall objectives of the future development of IMT for 2020 and beyond," Recommendation ITU-R M.2083-0, September 2015 (hereafter, *IMT-2020 Recommendation*), pp. 1 and 11-12. Fixed wireless access is often referenced in the literature as a fourth use case, as discussed below. See Kai Korschelt *et al.*, "Entering the 5G cycle," *Canaccord Genuity Global Equity Research*, October 1, 2018 (hereafter, *Korschelt et al.-Cannacord 10/1/2018*), p. 6.

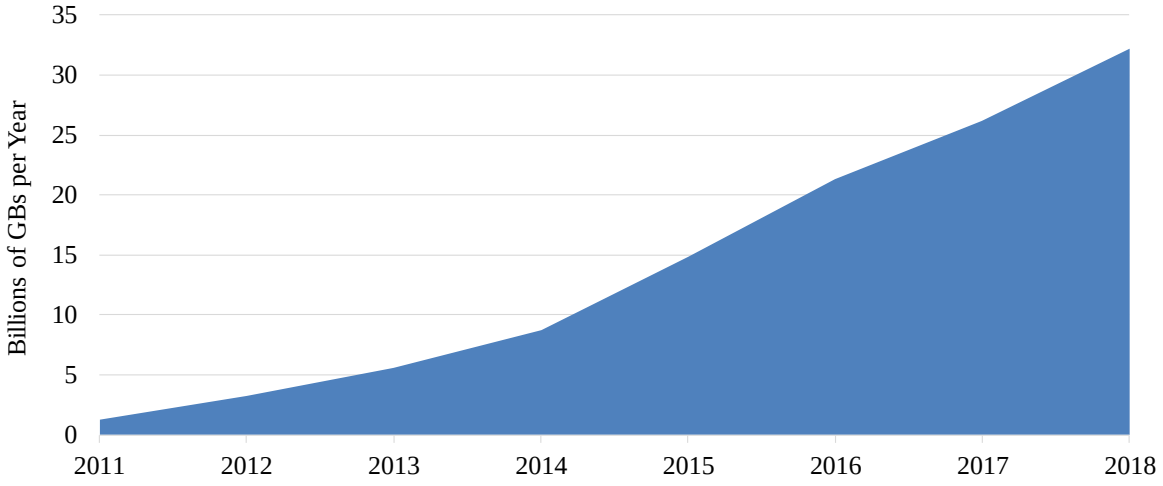
[72] See "Understanding mobile network experience: What do Opensignal's metrics mean?" *Opensignal Insights*, at https://www.opensignal.com/blog/2019/01/03/understanding-mobile-network-experience-what-do-opensignals-metrics-mean.

[73] See "Network capacity – definition," *GSMArena*, at https://www.gsmarena.com/glossary.php3?term=network-capacity.

[74] *IMT-2020 Recommendation*, p. 11.

56. Mobile data traffic in North America has increased by approximately 58 percent every year from 2011 to 2018.[75] Figure IV.2 shows the rapid rise of mobile traffic in the North America in just this decade. As data traffic increases, carriers must continually increase the capacity in their wireless networks if they are to handle the increased data load at acceptable quality levels. They can increase the capacity of their networks by increasing the number of cell sites and/or by increasing the capacity of the existing cell sites. McKinsey & Company projects that without purchasing new spectrum or increasing the number of cell sites, at least one carrier in the United States would run out of capacity on at least 50 percent of its cell sites by 2020.[76]

Figure IV.2
Mobile Data Traffic - North America, 2011-2018



Source: "Mobile data traffic," *Ericsson Mobility Visualizer*, at https://www.ericsson.com/en/mobility-report/mobility-visualizer?f=7&ft=2&r=4&t=8&s=4&u=3&y=2011,2018&c=3.

57. The 5G enhancement, eMBB, will support 100 times more traffic than does 4G technology and will increase peak speeds from 1 gigabit per second ("Gbps") to 20 Gbps.[77] Capacity

[75] "Mobile data traffic," Ericsson Mobility Visualizer, at https://www.ericsson.com/en/mobility-report/mobility-visualizer?f=7&ft=2&r=1&t=1,20&s=4&u=3&y=2011,2024&c=3.

[76] Ferry Grijpink *et al.*, "The road to 5G: The inevitable growth of infrastructure cost," *McKinsey & Company*, February 2018, at https://www.mckinsey.com/industries/telecommunications/our-insights/the-road-to-5g-the-inevitable-growth-of-infrastructure-cost.

[77] *IMT-2020 Recommendation*, pp. 11, 13-14.

improvements will enable the network to carry massive numbers of connections simultaneously[78] and will also help support ever-increasing data usage. 5G is also predicted to lower the cost per gigabyte ("GB") of data substantially.[79]

58. In addition, 5G will allow devices to communicate in almost real time, with latency as low as one tenth that of 4G.[80]

59. Higher speeds and lower latency will improve customers' experiences with current applications and uses, such as watching videos, surfing the internet, and engaging with social media. Higher speeds and lower latency will also undoubtedly engender newer technologies like augmented and virtual reality, 8K (ultra-high definition) video, new forms of social media,[81] and other applications and technologies that are not yet anticipated.

60. The second application of 5G is massive machine type communications ("mMTC"). This is a category of services for vast numbers of IoT devices that do not require high speeds but do require high connection density.[82] mMTC will support at least one million devices for every square kilometer.[83] Examples of mMTC devices include actuators, remote sensors, and equipment monitors.[84] Municipalities can use these mMTC devices to monitor a variety of factors, from trash levels to the flow of traffic on a street. The data can be used to save energy on lighting empty streets or on routing public transit.[85]

61. Another highly anticipated benefit of mMTC is energy efficiency gained through "smart grids."[86] Smart grids can measure real-time power demands instead of relying on

---

[78] Mark Collins *et al.*, "Are you ready for 5G?" February 2018, *McKinsey & Company*, at https://www.mckinsey.com/industries/telecommunications/our-insights/are-you-ready-for-5g.

[79] "The 5G Consumer Business Case. An economic study of enhanced mobile broadband," *Ericsson*, 2018, pp. 2, 7, at https://www.ericsson.com/assets/local/networks/documents/the-5g-consumer-business-case.pdf.

[80] *IMT-2020 Recommendation*, pp. 14-15.

[81] "5G Top 10 Use Cases," *Huawei Technologies Inc.*, at https://www.huawei.com/us/industry-insights/outlook/mobile-broadband/xlabs/use-cases/5g-top-10-use-case; Geoffrey Morrison, "TV resolution confusion: 1080p, 2K, UHD, 4K, 8K, and what they all mean," *CNET*, February 7, 2019, at https://www.cnet.com/news/4k-1080p-2k-uhd-8k-tv-resolutions-explained/.

[82] *IMT-2020 Recommendation*, pp. 12, 15.

[83] *IMT-2020 Recommendation*, p. 14.

[84] *Dahlman et al. 2018*, p. 4.

[85] "5G in 360," *CTIA*, at https://www.ctia5gin360.org/360/.

[86] "5G and Energy," 5G-Infrastructure-Association, September 30, 2015, pp. 3, 12, and 36.

inefficient predictive models and are expected to lead to "improved power quality, fewer power outages, smaller power outage areas, and easier grid deployments with less environmental impact in urban areas."[87] Analysts estimate that smart grids could generate $1.8 trillion in efficiency savings, thus saving consumers hundreds of dollars every year.[88]

62. In the healthcare sector, it is expected that mMTC will be used to monitor chronic illnesses and communicate with patients remotely. Goldman Sachs estimates that mMTC could save the United States $305 billion a year by curbing preventable healthcare costs.[89]

63. The third category of 5G applications is known as ultra-reliable and low latency communications ("URLLC").[90] Services that require low latency and high reliability include traffic safety, self-driving cars, and factory automation.[91] Deloitte, a global professional services firm, estimates that self-driving cars could reduce pollution emissions by 40-90 percent, reduce the average cost per passenger mile by 70 percent, and save 100 billion hours of productivity currently lost to driving.[92] A study by the Eno Center for Transportation predicts that if 90 percent of the vehicles in the United States were self-driving, 21.7 thousand lives and 447.1 billion dollars would be saved annually in the United States.[93]

64. A fourth category of 5G use is FWA, which will allow provision of "last mile" high-speed broadband service to residential and business customers over the wireless network. FWA is considered a more cost-effective alternative to fixed broadband provision in many areas.[94] "Last mile" deployment of wireline broadband (i.e., the wireline connections from neighbourhood or regional network nodes to customers' homes or offices) can be

---

[87] "5G and Energy," 5G-Infrastructure-Association, September 30, 2015, pp. 15 and 17.

[88] "Industry Data," *CTIA*, at https://www.ctia.org/the-wireless-industry/infographics-library?topic=17.

[89] David H. Roman and Kyle D. Conlee, "The Digital Revolution comes to US Healthcare: Technology, incentives align to shake up the status quo," *Goldman Sachs Global Investment Research*, June 29, 2015, pp, 4, 7.

[90] *IMT-2020 Recommendation*, pp. 11-12.

[91] *IMT-2020 Recommendation*, pp. 11-12.

[92] Scott Corwin *et al.*, "The future of mobility: How transportation technology and social trends are creating a new business ecosystem," *Deloitte University Press*, 2017, pp. 6, 19.

[93] "Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations," *Eno Center for Transportation*, October 2013, p. 8.

[94] *Korschelt et al.-Cannacord 10/1/2018*, p. 6.

prohibitively expensive, especially in rural areas. Compared to wireline alternatives such as fiber-to-the-home ("FTTH"), FWA has significantly lower capital expenditures, can be deployed quickly, and has lower operating expenditures.[95]

65. Globally, initial 5G applications are anticipated to be eMBB and FWA. mMTC and URLLC are anticipated to gain scale at a later stage.[96] However, as noted earlier, initial 5G applications in the United States are predominantly FWA and not eMBB.[97] I discuss the reason that U.S. deployment is following a different path from the rest of the world in the next section.

V. THE SPECTRUM "GAP" IN THE UNITED STATES

A. U.S. Policy Regarding 5G Deployment

66. The FCC declared the importance of broadband infrastructure in its 2010 National Broadband Plan:

> Like electricity a century ago, broadband is a foundation for economic growth, job creation, global competitiveness and a better way of life. It is enabling entire new industries and unlocking vast new possibilities for existing ones. It is changing how we educate children, deliver health care, manage energy, ensure public safety, engage government, and access, organize and disseminate knowledge.[98]

67. Ajit Pai, the current Chairman of the FCC, identified wireless innovation, and ensuring the U.S. leadership in it, as one of the agency's top priorities.[99]

68. Indeed, the FCC considers it important that the United States "win the race" to implement 5G:

---

[95] Korschelt et al.-Cannacord 10/1/2018, p. 6.

[96] "The promise and potential of 5G: Evolution or revolution?" IHS Markit, 2019, p. 7; 2019 Global Race to 5G Analysys Mason Report, p. 3.

[97] 2019 Global Race to 5G Analysys Mason Report, p. 3.

[98] "Connecting America: The National Broadband Plan," The Federal Communications Commission, March 17, 2010, p. XI.

[99] See Ajit Pai's video speech at "The FCC's 5G FAST Plan," FCC, at https://www.fcc.gov/5G.

> America is in the midst of a transition to the next generation of wireless services, known as 5G. These new services can unleash a new wave of entrepreneurship, innovation, and economic opportunity for communities across the country. The FCC is committed to doing our part to help ensure the United States wins the global race to 5G to the benefit of all Americans.[100]

69. However, the United States is not the only country that aspires to be a leader in 5G. Countries and carriers are competing vigorously to be the first to offer commercial 5G networks. Analysys Mason, a consulting and research company specializing in telecommunications, media, and technology,[101] anticipates that around 80 operators in more than 40 countries will make 5G services available to their subscribers by 2020.[102]

B. The State of 5G Deployment in the United States and the Rest of the World

i. Key Spectrum Bands Are Currently Unavailable to Carriers in the United States

70. The United States faces challenges to timely 5G deployment that other countries do not face. Specifically, the United States currently lacks available spectrum suitable for broad deployment of 5G, because the relevant spectrum has already been allocated by the FCC for other uses.[103]

---

[100] Declaratory Ruling and Third Report and Order, In the Matter of Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment; and Accelerating Wireline Broadband Deployment by Removing Barriers to Infrastructure Investment, Before the Federal Communications Commission, WT Docket No. 17-79; and WC Docket No. 17-84, FCC 18-133 (Released: September 27, 2018), ¶ 1.

[101] "About Us," Analysys Mason, at http://www.analysysmason.com/About-Us/Who-we-are/.

[102] 2019 Global Race to 5G Analysys Mason Report, p. 1.

[103] "FCC Online Table of Frequency Allocations," 47 C.F.R. § 2.106, Federal Communications Commission, Office of Engineering and Technology, Policy and Rules Division, revised on May 7, 2019, at https://transition.fcc.gov/oet/spectrum/table/fcctable.pdf.

71. As with any wireless service, spectrum is essential for 5G deployment.[104] To deploy commercial mobile 5G networks on a nationwide and, ultimately, ubiquitous basis, it is generally understood that carriers need low-, mid-, and high-band spectrum.[105]

72. Due to its physical properties, low-band spectrum—frequencies below 3 GHz[106]—can travel long distances and reach indoors. Low-band spectrum is currently considered necessary to economically provide 5G coverage in suburban and rural areas.[107] However, low-band spectrum does not offer the same high speeds that can be achieved with 5G deployment in mid-band and high-band spectrum for two reasons. First, the speed available in 5G depends on the width of the available spectrum, and available bandwidths in low-band spectrum are relatively narrow.[108] Second, massive MIMO technology, a key component of 5G that drives its speed and efficiency (discussed at length in Section VII.C

---

[104] Spectrum is a necessary input into wireless service. Wireless voice and data services are provided "through the air" via the electromagnetic spectrum, from a user's wireless device to a nearby communications tower and vice versa. Radio spectrum is a range of the electromagnetic spectrum. Radio spectrum at frequencies from 3 kilohertz ("kHz") to 300 gigahertz ("GHz") is used to transmit sound, data, and video. Radio spectrum allows the transmission of voice communications to and from cell phones, television signals from broadcasters' antennas to consumers' televisions, radio signals from radio broadcast antennas to consumers' AM and FM radios, and data communications such as internet web sites, music, photos, and video to and from smartphones. U.S. Government Accountability Office, "Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available," GAO-18-71, November 2017, footnote 1, p. 1 and note to Figure 2, p. 8; Marguerite Reardon, "Wireless spectrum: What it is, and why you should care," CNET, August 13, 2012, at https://www.cnet.com/news/wireless-spectrum-what-it-is-and-why-you-should-care/; and Mike Freeman, "Too much mobile data, not enough airwaves," *The San Diego Union-Tribune*, August 11, 2013, at http://www.sandiegouniontribune.com/business/technology/sdut-Spectrum-Qualcomm-mobile-data-smartphones-tablets-2013aug11-htmlstory.html.

[105] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, p. 2.

[106] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, p. 2.

[107] "A National Spectrum Strategy to Lead in 5G," *CTIA*, pp. 5-6.

[108] "Professor Rappaport Explains Why T-Mobile 5G 600 MHz Ultimately Doesn't Make It," Wireless One, May 3, 2018, at http://wirelessone.news/10-r/1037-professor-rappaport-explains-why-t-mobile-5g-600-mhz-are-a-dud. Theodore Rappaport serves as the David Lee/Ernst Weber Professor of Electrical Engineering at New York University's ("NYU") Tandon School of Engineering, a professor of computer science at the NYU Courant Institute of Mathematical Sciences, and a professor of radiology at the NYU School of Medicine. See "Faculty: Theodore Rappaport," NYU Tandon School of Engineering, Polytechnic Institute, at https://engineering.nyu.edu/faculty/theodore-rappaport. "5G Spectrum Vision," 5G Americas Whitepaper, p. 17, at http://www.5gamericas.org/files/4015/4958/3330/5G_Americas_5G_Spectrum_Vision_Whitepaper.pdf; Berge Ayvazian, Fred Campbell, and Haig Sarkissian, "Spectrum Strategies for 5G: 2019 Update." Wireless 20|20, January 2019, p. 5, at http://www.wireless2020.com/media/white-papers/Spectrum-Strategies-for-5G-2019-Update.pdf.

below), is not currently feasible in low-band spectrum because the long wavelengths of low-band spectrum require antennas that are too large to fit into massive MIMO arrays.[109]

73. High-band spectrum—spectrum at frequencies above 24 GHz,[110] also known as millimeter wave ("mmW") spectrum—is important for high-speed and high-capacity applications. High-band spectrum waves, however, have poor propagation characteristics relative to lower frequency bands with respect to distance and ability to penetrate obstacles.[111] Hence, it is generally considered uneconomic to deploy 5G using mmW spectrum for mobile applications in any but the most densely populated areas, such as central metro areas, transportation centers (e.g., airports), and event locations (e.g., stadiums).[112] Even in these densely populated areas, 5G deployed in mmW spectrum is not projected to cover entire large central metro areas. Instead, it is projected to be selectively deployed in densely populated areas to provide adequate data capacity.[113]

74. Mid-band spectrum (spectrum at frequencies between 3 and 24 GHz[114]) is called a "key building block" for 5G.[115] Its physical properties provide mid-band spectrum with good coverage and high capacity, making it the most suitable spectrum band for economic deployment of 5G in urban areas.[116] Countries such as Japan, South Korea, Spain, China,

---

[109] "Professor Rappaport Explains Why T-Mobile 5G 600 MHz Ultimately Doesn't Make It," Wireless One, May 3, 2018, at http://wirelessone.news/10-r/1037-professor-rappaport-explains-why-t-mobile-5g-600-mhz-are-a-dud.

[110] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, p. 2.

[111] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, p. 2.

[112] David Sosa and Greg Rafert, "The Economic Impacts of Reallocating High-Band Spectrum to 5G in the United States," *Analysis Group*, April 2019, pp. 2, 11-12.

[113] David Sosa and Greg Rafert, "The Economic Impacts of Reallocating High-Band Spectrum to 5G in the United States," *Analysis Group*, April 2019, pp. 11-12.

[114] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, p. 2.

[115] "A National Spectrum Strategy to Lead in 5G," *CTIA*, p. 6.

[116] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, p. 2.

Switzerland, and the United Kingdom have been focusing on mid-band spectrum for 5G deployment.[117]

75. According to Analysys Mason, mid-band spectrum is essential for the U.S. 5G commercial launch:

> Many of the planned 5G commercial launches referred to in our report will use mid-band spectrum…The US has previously lagged behind other nations in terms of the amount of mid-band spectrum being released for 5G use. Whilst there has been significant progress in the US on other important aspects of 5G launch, such as reform of infrastructure planning procedures (e.g. in relation to small-cell siting), there is still more to be done to ensure that the US retains its leading position through better availability of mid-band spectrum, which is a key short-term goal.[118]

76. Data on sales of RAN equipment show that 5G RAN equipment for sub-6 GHz technology (i.e., technology that operates in low- and mid-spectrum bands between 450 MHz and 6 GHz[119]) accounted for approximately 95 percent of total 5G RAN sales in Q4 2018-Q1 2019 worldwide.[120] Revenue from mmW (i.e., 5G RAN that operates in high-band spectrum bands between 24.25 GHz and 52.60 GHz[121]) technology equipment was much smaller—approximately 5 percent of total global 5G RAN equipment revenues. These data also confirm that only a small fraction of deployments use equipment operating in high-band spectrum.

---

[117] "A National Spectrum Strategy to Lead in 5G," *CTIA*, p. 6; Anne Morris, "Swisscom Readies for Europe's First Commercial 5G Launch With Phones," *SDX Central*, April 10, 2019, at https://www.sdxcentral.com/articles/news/swisscom-readies-for-europes-first-commercial-5g-launch-with-phones/2019/04/; "MIIT awards 5G licences to three MNOs plus cable operator," *TeleGeography*, June 6, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/06/06/miit-awards-5g-licences-to-three-mnos-plus-cable-operator/index.html.

[118] *2019 Global Race to 5G Analysys Mason Report*, p. 2.

[119] See 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 15 Description; Summary of Rel-15 Work Items (Release 15), TR 21.915 v1.0.0 (2019-03), p. 29.

[120] See "MOBILE RADIO ACCESS NETWORK – 5G NR – Sub 6 GHz" and "TOTAL 5G NR," Dell'Oro Group, Q1 2019.

[121] See 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 15 Description; Summary of Rel-15 Work Items (Release 15), TR 21.915 v1.0.0 (2019-03), p. 29.

77. FCC Chairman Ajit Pai called mid-band spectrum "important" for deployment of 5G in the United States.[122] The FCC identified three mid-bands for 5G networks buildout: 3.5 GHz, 3.7-4.2 GHz, and 2.5 GHz bands.[123] The U.S. Department of Commerce's National Telecommunications and Information Administration ("NTIA") additionally identified the 3.45-3.55 GHz band as a band that could potentially be repurposed for commercial wireless use.[124]

78. The United States is unique in spectrum allocation. In the United States, low- and high-band spectrum has been allocated for mobile use, but other than the mid-band spectrum in 2.5 GHz bands available to only Sprint, [125] mid-band spectrum has not been made available for mobile use.[126] As of June 2019, the 3.45-3.55 GHz, 3.5 GHz, and 3.7-4.2 GHz bands were unavailable to U.S. carriers, and the auctions of these spectrum bands had yet to be

[122] Statement of Chairman Ajit Pai, Federal Communications Commission, Hearing on "Oversight of the Federal Communications Commission," Before the United States Senate Committee on Commerce, Science, and Transportation, June 12, 2019, available at https://docs.fcc.gov/public/attachments/DOC-357959A1.pdf.

[123] Note that while many sources categorize 2.5 GHz band as a low-band, the FCC categorizes it as a mid-band. See "The FCC's 5G FAST Plan," *FCC*, at https://www.fcc.gov/5G; *2019 Global Race to 5G Analysys Mason Report*, p. 23. Similar to the FCC, I refer to 2.5 GHz bands as a mid-band in this report.

[124] "5G Spectrum Vision," *5G Americas Whitepaper*, February 2019, p. 7.

[125] "Sprint Lights Up True Mobile 5G in Atlanta, Dallas-Fort Worth, Houston and Kansas City," Sprint Press Release, May 30, 2019, at https://newsroom.sprint.com/sprint-lights-up-true-mobile-5g-in-atlanta-dallas-fort-worth-houston-and-kansas-city.htm.

[126] *2019 Global Race to 5G Analysys Mason Report*, Figures 4.1, 4.4, and 4.7.

scheduled.[127] Sprint, moreover, does not have sufficient low- or any high-band spectrum necessary for nationwide 5G deployment.[128,129]

79. The United States is therefore at a material disadvantage in competing for leadership in 5G deployment with countries in which mid-band spectrum has already been allocated (e.g., China, Japan, and South Korea[130]), while in the United States mid-band spectrum is unavailable to three of the four top carriers and no clear timeline for its allocation has been established. I refer to this situation as the U.S. "spectrum gap."

ii. The United States Is Currently Well Behind Other Countries in 5G Deployments

80. Despite the lack of adequate mid-band spectrum in the United States, all four major U.S. carriers have announced plans for 5G deployment. All four carriers had launched commercial 5G networks at the time of this report.[131]

81. Verizon, T-Mobile, and AT&T have launched their networks in mmW spectrum (28 GHz and 39 GHz); Sprint is using its 2.5 GHz mid-band spectrum for its 5G network.[132]

---

[127] 2019 Global Race to 5G Analysys Mason Report, Figure 4.5.

[128] Sprint does not have low-band spectrum available for 5G deployment. See John Saw, "Winning the Global Race to 5G," Sprint, April 4, 2019 at https://newsroom.sprint.com/winning-global-race-to-5g.htm. Sprint does not own licenses for high-band spectrum. See Mike Dano, "Special Report – 25 charts on spectrum ownership in the United States," FierceWireless, July 12, 2018, at https://www.fiercewireless.com/wireless/25-charts-spectrum-ownership-united-states; Joan Engebretson, "5G Millimeter Wave Auction Winners: AT&T, T-Mobile, Verizon, Windstream, Starry, and Others," Telecompetitor, June 3, 2019, at https://www.telecompetitor.com/5g-millimeter-wave-auction-winners-att-t-mobile-verizon-windstream-starry-and-others/.

[129] A merger between Sprint and T-Mobile was approved on June 26, 2019 by the U.S. Department of Justice. When Sprint and T-Mobile merge, the merged company will combine low- and high-band spectrum owned by T-Mobile with mid-band spectrum owned by Sprint to become the only U.S. carrier with all three spectrum bands necessary for nationwide 5G deployment. Sprint and T-Mobile project that the combination of T-Mobile's low- and high-band spectrum and Sprint's mid-band spectrum will deliver over 400 MHz of spectrum, improving the capacity that standalone Sprint and T-Mobile offer today, combined, by a factor of eight. See, "T-Mobile and Sprint Receive Clearance from Department of Justice for Merger to Create the New T-Mobile," T-Mobile Press Release, June 26, 2019, at https://investor.t-mobile.com/news-and-events/t-mobile-us-press-releases/press-release-details/2019/T-Mobile-and-Sprint-Receive-Clearance-from-Department-of-Justice-for-Merger-to-Create-the-New-T-Mobile/default.aspx; "Leading the 5G For All Revolution," T-Mobile and Sprint, at https://newtmobile.com/leading-the-5g-revolution/.

[130] 2019 Global Race to 5G Analysys Mason Report, Figure 4.4.

[131] See Appendix D.

[132] See Appendix D.

82. Nevertheless, data show that despite the efforts of the U.S. carriers to deploy in available spectrum bands, the United States is well behind Asia in 5G deployment.

83. Dell'Oro data indicate that the highest spending on 5G RAN in Q4 2018-Q1 2019, the first two quarters that record data on 5G RAN spending, occurred in North America and Asia Pacific. The majority of all global spending on 5G RAN equipment in these two quarters was in Asia, which exceeded spending on 5G RAN equipment in North America by a factor of three.

84. As detailed in Appendix D, carriers in other counties have launched commercial 5G networks using mid-band spectrum. These include Sunrise and Swisscom in Switzerland and SK Telecom, KT, and LG Uplus in South Korea.[133]

85. Japan, China, and the UAE have not yet launched commercial 5G services but have made significant progress in 5G deployment.[134] While China has not yet launched a commercial 5G network, some analyst reports identify China as a leader in the "race" to 5G implementation. China's record of rapid network deployment, committed funds to 5G-related investment, strong government and industry backing, extensive testing, and availability of large amounts of mid-band spectrum contribute to China's leading position.[135] Chinese carriers were granted 5G spectrum licenses a year ahead of China's initial schedule, accelerating 5G network rollouts.[136]

---

[133] See Appendix D.

[134] See Appendix D.

[135] Deloitte highlighted China's rapid network densification since 2015, which is important for 5G, and China's five-year economic plan that allocates $400 billion for 5G-related investment. Based on these two criteria, Deloitte identified China as one of the leaders in 5G race. Dan Littman *et al.*, "5G: The chance to lead for a decade," *Deloitte*, 2018, pp. 1, 4-5. Analysys Mason found that China and the United States were leaders in terms of 5G readiness in spring of 2019. The earliest 5G rollout in China is projected to start in Q4 2019. See *2019 Global Race to 5G Analysys Mason Report*, pp. 1, 25-26, 56, 64, and 66; Appendix D.

[136] Mike Dano, "China Finally Lights Its 5G Fire," *Light Reading*, June 6, 2019, at https://www.lightreading.com/mobile/5g/china-finally-lights-its-5g-fire/d/d-id/752001.

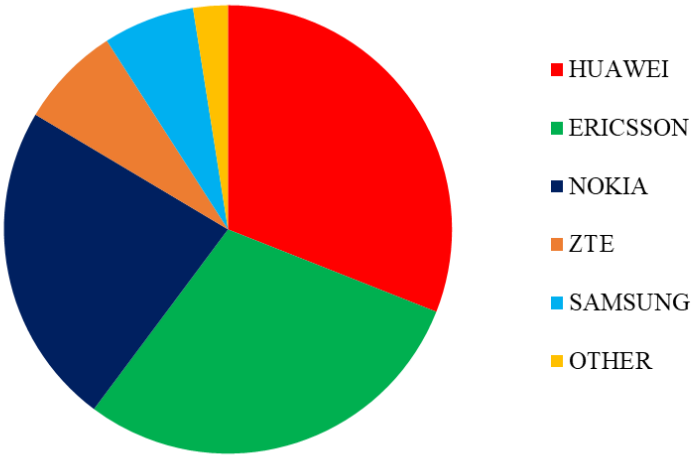
VI. THE MARKET FOR RAN NETWORK EQUIPMENT IN THE UNITED STATES AND THE REST OF THE WORLD

86. The development and manufacture of RAN equipment for new technologies is highly complex, requiring substantial R&D investment, expertise, and experience. There are only five companies in the world that have the capabilities to participate meaningfully in the RAN market. They are Huawei, Telefonaktiebolaget LM Ericsson ("Ericsson"), Nokia Corporation ("Nokia"), Samsung Electronics Co., Ltd. ("Samsung"), and ZTE Corporation ("ZTE").[137] Profiles of the five major RAN equipment vendors are provided in Appendix A.

87. Huawei is the leading provider of RAN equipment worldwide. Figure VI.1 shows vendor revenue shares of RAN equipment for all technologies in 2018. As the figure shows, approximately one-third of all RAN equipment spending worldwide was on Huawei equipment. Huawei had the largest revenue share in the market for RAN equipment worldwide in 2018.

[137] Other significant competitors that existed in the last decade include Nortel Networks (whose wireless technologies unit was auctioned to Ericsson in bankruptcy proceedings in 2009), Motorola Solutions (the majority of whose wireless network infrastructure assets were acquired by Nokia in April 2011), and Alcatel-Lucent (which was acquired by Nokia in January 2016). See Ian Austen, "Ericsson Wins Auction for Nortel Assets," *The New York Times*, July 26, 2009, at https://www.nytimes.com/2009/07/27/technology/companies/27iht-nortel.html; Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2012, p. 48; Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2014, p. 5.

Figure VI.1
Revenue Shares of RAN Equipment Vendors - Worldwide, 2018



Note: These data include sales of GSM, CDMA, WCDMA, LTE, and 5G RAN equipment.

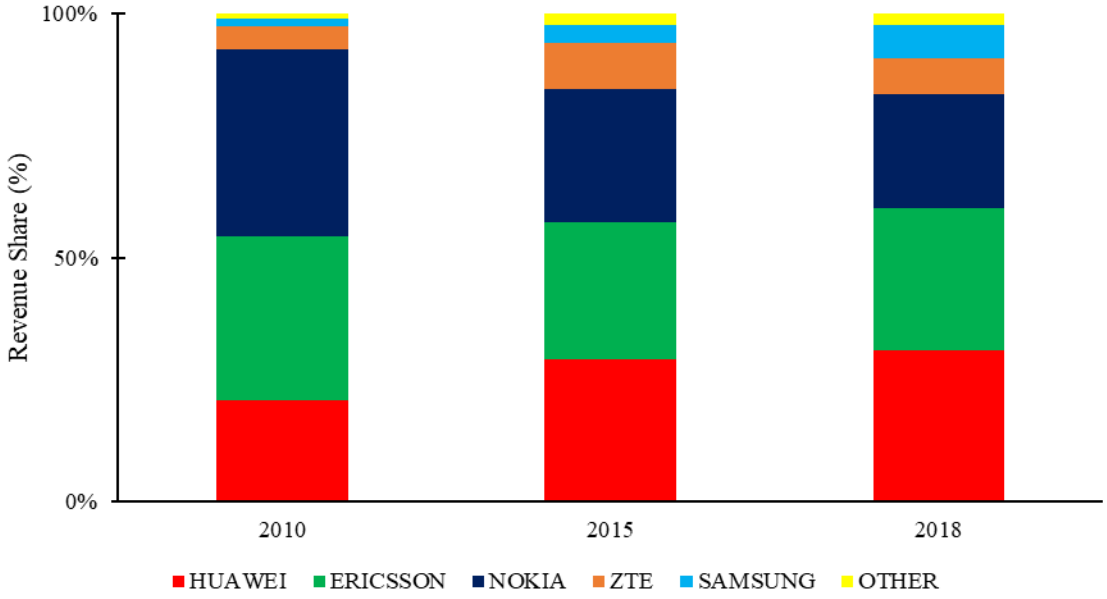
Source: "TOTAL MOBILE RADIO ACCESS NETWORK (GSM+CDMA+WCDMA+WiMAX+LTE+5G NR)," Dell'Oro Group, Q1 2019.

88. Figure VI.1 also shows that Ericsson and Nokia capture the majority of sales outside of Huawei, and Samsung and ZTE also have material, although smaller, volumes of sales of RAN equipment.

89. Figure VI.2 shows the revenue shares of the top five providers of RAN equipment worldwide for each year in 2010, 2015, and 2018. Huawei has been the leading provider of RAN equipment globally since 2015, despite the fact that Huawei has never had a material presence in the U.S. market.[138] The figure and data also show that Nokia's aggregated RAN sales share worldwide has been declining in recent years and Ericsson's aggregated RAN sales share has been approximately flat in recent years, while the revenue shares of Huawei and Samsung have been increasing. The revenue share of ZTE increased from 2013 through 2016, but it has been declining over the last two years.

[138] Huawei's revenue share in the North American region, which includes the United States and Canada, has been consistently low over this period.

Figure VI.2
Revenue Shares of Top 5 RAN Equipment Vendors – Worldwide, 2010, 2015, and 2018



Note: Nokia acquired the wireless networks business of Panasonic Systems Networks Company Limited in January 2015, and Alcatel-Lucent in January 2016. I include all three companies' revenues in the calculation of Nokia's revenue shares.

Source:
[1] TOTAL MOBILE RADIO ACCESS NETWORK (GSM+CDMA+WCDMA+WiMAX+LTE+5G NR)," Dell'Oro Group, Q1 2019.
[2] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2014, p. 5.
[3] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2016, p. 2.

90. Huawei's global leadership in RAN equipment spans the most advanced countries and less developed countries. Huawei had the highest revenue share of RAN equipment in Europe, Asia Pacific, and the Middle East and Africa in 2018, and had the second-largest revenue share in the Caribbean and Latin America ("CALA"). The broad acceptance and use of Huawei's RAN equipment evidences the respect for Huawei's technology throughout the world.

91. Huawei reported to the FCC that its multinational operations support more than 500 major telecommunications operators across more than 170 countries. It also reported that in mid-

2018 it served 45 out of world's 50 largest telecommunications providers.[139] As of 2016, Huawei supplied more than half of the 537 4G networks globally and 59 of the 90 4.5G networks[140] globally.[141]

92. Clearly, carriers around the world, including those in countries operating the world's most advanced networks, have found Huawei equipment to present a compelling technological solution and attractive value proposition.

93. As Huawei's revenue share has increased around the world, however, its position in the United States has been stunted. Huawei entered the North American market in 2008, but since then its revenue share in all RAN equipment has been consistently low in each year.[142] In 2010, eight senators asked the president to intervene when Huawei attempted to bid to provide telecommunications equipment to Sprint Nextel, a major U.S. carrier at the time.[143] This bid was excluded by Sprint Nextel largely due to national security concerns.[144] Softbank Group Corp, a Japanese information industry company that acquired Sprint Nextel in 2013,[145] promised U.S. authorities to remove Huawei's equipment from Sprint Nextel's newly acquired Clearwire Corp networks.[146] In addition, in 2011, the U.S. House

---

[139] Comments of Huawei Technologies Co., LTD and Huawei Technologies USA, Inc., *In the Matter of Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Before the Federal Communications Commission, Washington, D.C., 20554, WC Docket No. 18-89, June 1, 2018, p. 5.

[140] LTE-Advanced Pro, also known as 4.5G, is a set of 3GPP-approved technologies that bring LTE capabilities closer to 5G. LTE-Advanced Pro offers lower latency, improved reliability, and higher speeds compared to the previous technology generations. See Zhou Dongfei, "On the path to 5G with 4.5G," Huawei, October 18, 2016, at https://www.huawei.com/en/about-huawei/publications/communicate/80/reaching-5g-with-45g.

[141] "China's Huawei set to lead global roll-out of 5G mobile networks," *South China Morning Post*, February 23, 2018, at https://www.scmp.com/tech/enterprises/article/2134498/chinas-huawei-set-lead-global-roll-out-5g-mobile-networks.

[142] "TOTAL MOBILE RADIO ACCESS NETWORK (GSM+CDMA+WCDMA+WiMAX+LTE+5G NR)," Dell'Oro Group, Q1 2019.

[143] David Barboza, "Scrutiny for Chinese Telecom Bid," *The New York Times*, August 22, 2010, at https://www.nytimes.com/2010/08/23/business/global/23telecom.html.

[144] Joann S. Lublin and Shayndi Raice, "Security Fears Kill Chinese Bid in U.S," *Wall Street Journal*, November 5, 2010, at https://www.wsj.com/articles/SB10001424052748704353504575596611547810220.

[145] "Sprint and SoftBank Announce Completion of Merger," Sprint Press Release, July 10, 2013, at https://newsroom.sprint.com/sprint-and-softbank-announce-completion-of-merger.htm.

[146] Danny Yadron and Spencer E. Ante, "Sprint and Softbank Agree to Forgo, Remove Huawei Equipment, Lawmaker Says," *Wall Street Journal*, March 28, 2013, at https://blogs.wsj.com/washwire/2013/03/28/sprint-and-softbank-agree-to-forgo-remove-huawei-equipment-lawmaker-says/; Sprint Corporation, Form 10-K for the fiscal year ended December 31, 2013, pp. 2, 25.

of Representatives Permanent Select Committee on Intelligence initiated an investigation into Huawei and ZTE to "inquire into the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the United States."[147] The committee's report concluded that the United States should "view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies." It recommended placing restrictions on the use of Huawei's and ZTE's equipment by U.S. government systems and strongly encouraged private sector entities to seek vendors other than Huawei and ZTE for their projects.[148]

94. The NDAA for the Fiscal Year 2018, Section 1656, prohibited the procurement of Huawei's and ZTE's equipment for certain government uses, starting December 2018.[149] The NDAA for Fiscal Year 2019, Section 889, places additional restrictions on the procurement and use of Huawei's equipment by the government and federal contractors starting in August 2019.

95. As discussed above, Huawei's revenue share in North America is significantly lower than its revenue share in the rest of the world. In Dell'Oro Group's data, North America consists only of the United States and Canada. Because Canada is a small country (Canada has less than one-tenth the number of wireless subscriptions as the United States[150]), the data show that the major exception to Huawei's leading presence in RAN sales is the United States. Huawei's presence in the United States is primarily limited to serving small rural carriers.[151] Because the use of Huawei equipment was not restricted in Canada in 2018

[147] "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, U.S. House of Representatives, 112th Congress, October 8, 2012, p. iv.

[148] "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, U.S. House of Representatives, 112th Congress, October 8, 2012, p. 45.

[149] John S. McCain National Defense Authorization Act for Fiscal Year 2018, § 1656(b)(1) and (c).

[150] Canada had 31.693 million mobile cellular subscriptions in 2017, compared to 391.6 million subscriptions in the United States. 31,693,000/391,600,000 = 8.1 percent. See "Statistics: Mobile-cellular subscriptions," International Telecommunications Union, at https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx.

[151] Jeff Johnston, "Equipment Ban Creates Static for Rural Telecom Operators," CoBank, June 2019, p. 1.

and was used by two of Canada's three largest carriers,[152] it is likely that Huawei's revenue share in the United States in 2018 was even lower than its revenue share in North America.

96. In North America, sales are essentially split between Ericsson and Nokia. Samsung is the third largest vendor, with a much smaller share of revenues. ZTE, another Chinese company whose sales in the United States have been restricted by U.S. government policy, had no RAN sales in North America in 2018.

97. The countries that use Huawei network equipment have among the fastest networks in the world, while U.S. wireless network performance ranks poorly in a global comparison.

98. Opensignal, a leading company in measuring network coverage and performance, conducts ongoing studies of wireless network performance on a variety of metrics, including download speed and latency.[153] By Opensignal's metrics, the 4G networks in the United States currently rank 30th among nations in download speed, 39th in upload speed, and 50th in latency. In download speed, the 4G networks in the United States rank behind 21 European countries, 4 Asian countries, Australia, New Zealand, Qatar, and Canada.[154] The 4G networks in many (if not all) of the best-performing countries use Huawei equipment, including the top three in download speed: South Korea,[155] Norway,[156] and Canada.[157]

---

[152] See Josh Wingrove, "Canada Puts Huawei 5G Decision on Back Burner With Allies Split," May 8, 2019, *Bloomberg*, at https://www.bloomberg.com/news/articles/2019-05-08/canada-puts-huawei-5g-decision-on-back-burner-with-allies-split.

[153] "About us," Opensignal, at https://www.opensignal.com/about/about-us. See also, "Understanding mobile network experience: What do Opensignal's metrics mean?" *Opensignal Insights*, at https://www.opensignal.com/blog/2019/01/03/understanding-mobile-network-experience-what-do-opensignals-metrics-mean.

[154] Peter Boyland, "The State of Mobile Network Experience: Benchmarking mobile on the eve of the 5G revolution," Opensignal, May 2019, pp. 3 and 9, at https://www.opensignal.com/sites/opensignal-com/files/data/reports/global/data-2019-05/the_state_of_mobile_experience_may_2019_0.pdf.

[155] Collaborate to Commercially launch the World's First Uplink 2 CC CA Technology," Huawei Press Release, April 29, 2016, at https://www.huawei.com/en/press-events/news/2016/4/World-First-Uplink-2-CC-CA-Technology.http://english.chosun.com/site/data/html_dir/2019/06/18/2019061801409.html.

[156] Sveinung Sleire, "Norway Mulls Huawei 5G Decision That's Not 'Black and White'" *Bloomberg*, March 25, 2019, at https://www.bloomberg.com/news/articles/2019-03-25/norway-mulls-huawei-5g-decision-that-s-not-black-and-white.

[157] Mark Gollom, "Banning Huawei from building new 5G wireless network won't really hurt Canada's big telecom firms," *CBC News*, December 19, 2018, at https://www.cbc.ca/news/business/huawei-ban-government-bell-telus-5g-1.4950521.

99. The strong demand for Huawei's products across the globe is shown in RAN sales of 2G, 3G, and 4G equipment. Using the data provided to me by Dell'Oro Group, I calculated Huawei's revenue share of RAN sales by technology (i.e., GSM, CDMA, WCDMA, and LTE) and by region. The data show that in every region outside of North America, Huawei is a leading equipment provider in every technology. The data also show that although 5G deployment is nascent, in the regions where carriers have deployed 5G networks and where Huawei is not restricted (i.e., Europe, Middle East and Africa, and Asia Pacific), Huawei has a substantial (and often the largest) revenue share in 5G sales as well.[158]

100. Most of the 5G RAN revenues from deployment in Asia Pacific are likely from 5G deployments in South Korea,[159] and all or almost all 5G RAN revenues in North America are likely from the deployments of 5G in the United States.[160] In Q4 2018-Q1 2019 in Asia Pacific, Samsung had the highest revenue share from sales of 5G RAN equipment and Huawei had the second highest revenue share from sales of 5G RAN.

101. The available facts suggest that Samsung's success in Asia Pacific is due largely to success in its home country and is unlikely to be predictive of its future 5G RAN revenue shares in other countries and regions. The data also indicate that even in South Korea, Huawei had a substantial revenue share, and in other regions where 5G is being deployed and Huawei is allowed to supply 5G RAN equipment, Huawei had the largest revenue share.[161]

102. Huawei's global leadership in 5G RAN equipment is also reflected in the number of commercial contracts it holds for deployment of 5G networks, which are good predictors of future sales. Public reports indicate that as of June 2019, Huawei had won 50 5G commercial contracts in 30 countries and shipped 150,000 5G base stations.[162]

---

[158] These data are provided by Dell'Oro Group. Due to the confidentiality of these data, I am not able to publish the supporting data in this report.

[159] Only South Korea has launched 5G networks, and other countries in Asia Pacific that are close to deploying and launching 5G network only recently allocated spectrum for 5G. See Appendix D.

[160] No Canadian carrier has deployed a 5G network. See, Cindy Baker, "Mainstream launch of 5G expected in Canada in 2021," *IT World Canada*, May 2, 2019, at https://www.itworldcanada.com/article/mainstream-launch-of-5g-expected-in-canada-in-2021/417579.

[161] Based on the data provided by Dell'Oro Group.

[162] Sherisse Pham, "Huawei is still signing up 5G customers despite US Pressure," *CNN Business*, June 26, 2019, at https://www.cnn.com/2019/06/26/tech/huawei-ken-hu-mwc/index.html.

103. Huawei had won more 5G commercial contracts than its two main competitors, Ericsson and Nokia. Ericsson had won 21 5G commercial contracts as of June 2019, and Nokia had won 42 as of June 2019.[163] ZTE had won 25 5G commercial contracts as of June 2019.[164] No information on the number of 5G commercial contracts is available for Samsung.

104. Despite Nokia's large number of 5G commercial contracts, its revenues from the early 5G deployments are quite low compared to those of the other three vendors.[165] Nokia's relatively low revenues in context of its significant number of commercial contracts might be a consequence of the fact that Nokia was at least three months behind its scheduled equipment delivery to South Korea's three carriers.[166] News articles report that one of the carriers, KT, decided to replace Nokia equipment with Samsung equipment because of delays in Nokia's supply.[167] In addition, analysts reported quality problems with Nokia's 5G equipment related to data processing capacity, radio interferences, and dual connectivity. Some carriers found that the performance of Nokia's equipment was inferior to that of Samsung, Huawei, and Ericsson.[168] As a result, areas where Nokia's equipment is installed in South Korea were reported to be removed from 5G coverage maps.[169]

105. In the next section I will explain factors behind Huawei's success, including its industry-leading investments in R&D and experience developing and implementing technologies crucial to 5G deployment.

---

[163] "Live 5G networks and publicly announced 5G contracts," *Ericsson*, June 12, 2019, at https://www.ericsson.com/en/5g/5g-networks/5g-contracts; Sherisse Pham, "Nokia is fighting hard to steal Huawei's 5G crown," *CNN Business*, at https://edition.cnn.com/2019/06/04/tech/huawei-5g-nokia/index.html.

[164] "ZTE secures 25 5G commercial contracts," *Yahoo Finance*, June 25, 2019, at https://finance.yahoo.com/news/zte-secures-25-5g-commercial-063100842.html.

[165] Based on the data provided by Dell'Oro Group.

[166] Michael Herh, "Nokia Equipment Causes Trouble for Korea's 5G Service Providers," *Business Korea*, April 23, 2019, at http://www.businesskorea.co.kr/news/articleView.html?idxno=31165.

[167] Michael Herh, "Nokia Equipment Causes Trouble for Korea's 5G Service Providers," *Business Korea*, April 23, 2019, at http://www.businesskorea.co.kr/news/articleView.html?idxno=31165.

[168] Michael Herh, "Nokia Equipment Causes Trouble for Korea's 5G Service Providers," *Business Korea*, April 23, 2019, at http://www.businesskorea.co.kr/news/articleView.html?idxno=31165.

[169] Michael Herh, "Nokia Equipment Causes Trouble for Korea's 5G Service Providers," *Business Korea*, April 23, 2019, at http://www.businesskorea.co.kr/news/articleView.html?idxno=31165.

VII. HUAWEI HAS UNIQUE CHARACTERISTICS WHOSE CONTINUED ABSENCE WILL DELAY THE U.S. TRANSITION TO 5G

106. Huawei possesses a unique combination of characteristics among equipment vendors. Continued exclusion of Huawei from the U.S. market will likely impede and delay U.S. carriers' progress toward 5G deployment and 5G penetration.

107. Huawei provides unique value because of (1) its global leadership in R&D in terms of investment, patent production, and other measures of R&D; and (2) its leadership in key 5G technologies, especially Massive MIMO and the technologies that underlie Massive MIMO.

A. Huawei Is an R&D Leader in 5G

108. Huawei has invested more in total R&D spending than any other major network equipment vendor in every year since 2012.[170]

109. Huawei stated in its annual report that it has been heavily investing in 5G since 2009[171] and that innovation is one of its main priorities:

> Innovation and research are our lifeblood, and we will continue to invest over 10% of our annual revenue in R&D. In 2018 alone, our R&D investment exceeded 100 billion yuan, ranking fifth globally in *The 2018 EU Industrial R&D Investment Scoreboard*. Our continued investment has produced positive results, giving us the ability to provide our customers with innovative products and more efficient services.[172]

110. Figure VII.1 shows Ericsson's, Nokia's, and Huawei's R&D investment from 2009 through 2018. Huawei has invested more in total R&D spending than any other major network equipment vendor in every year since 2013 and has invested more than Ericsson and Nokia combined in each of the last four years.

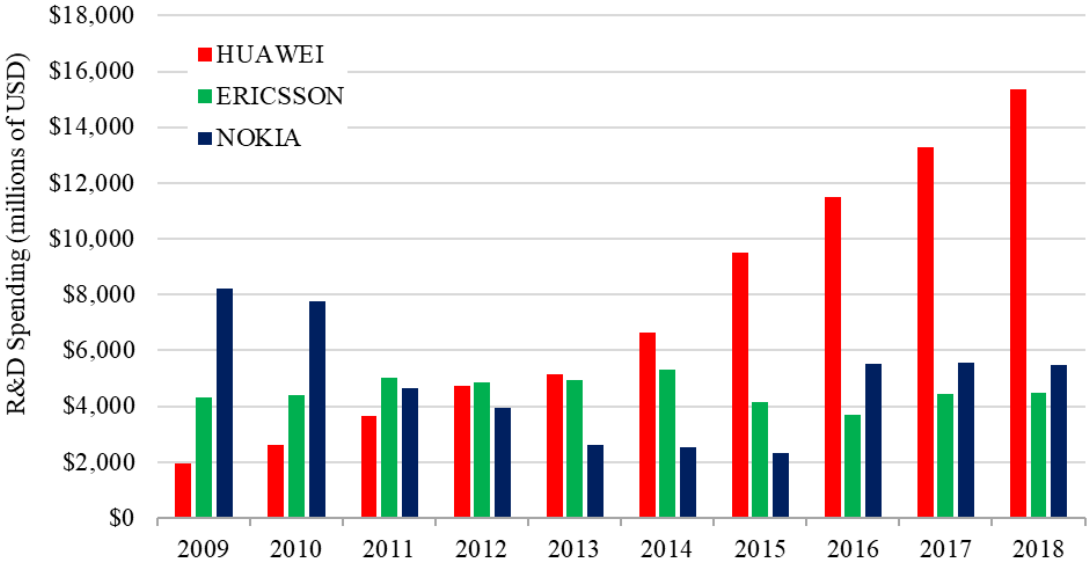
[170] Here I focus on R&D spending of the top three vendors. Based on their revenue shares in the market for RAN equipment, these are the only three carriers that have sufficient revenue shares to invest comparable amounts of resources in RAN R&D. See Figure VI.1.

[171] Huawei Investment & Holding Co., Ltd., 2017 Annual Report, p. 20.

[172] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 3.

111. The figure also shows that Huawei's R&D spending has been growing over the entire period, unlike the R&D investments of the other two vendors. Nokia's R&D investment declined overall from 2009 to 2018, and Ericsson's investment over the same period remained at approximately the same level, with small variations.

Figure VII.1
Total R&D Spending (in Millions) of Top 3 RAN Equipment Vendors, 2009-2018[173]



Note: Ericsson reports its research and development spending in millions of Swedish kronor (SEK). Nokia reports its research and development spending in millions of euros (EUR). Huawei reports its research and development spending in millions of Chinese yuan (CNY). I converted all research and development spending data into millions of U.S. dollars (USD), using annual exchange rates.

112. In 2018, the Scoreboard, the European Commission's report on companies' R&D spending, ranked Huawei among the top 3 ICT producers by R&D in the world and among

[173] "Sweden / U.S. Foreign Exchange Rate, Swedish Kronor to One U.S. Dollar, Annual, Not Seasonally Adjusted," Federal Reserve Bank of St. Louis, accessed July 29, 2019, at https://fred.stlouisfed.org/series/DEXSDUS#; "U.S. / Euro Foreign Exchange Rate, U.S. Dollars to One Euro, Annual, Not Seasonally Adjusted," Federal Reserve Bank of St. Louis, accessed July 29, 2019, at https://fred.stlouisfed.org/series/DEXUSEU#; "China / U.S. Foreign Exchange Rate, Chinese Yuan to One U.S. Dollar, Annual, Not Seasonally Adjusted," Federal Reserve Bank of St. Louis, accessed July 29, 2019, at https://fred.stlouisfed.org/series/DEXCHUS#; Telefonaktiebolaget LM Ericsson, 2011 Annual Report, p. 46; Telefonaktiebolaget LM Ericsson, 2012 Annual Report, p. 48; Telefonaktiebolaget LM Ericsson, 2013 Annual Report, p. 51; Telefonaktiebolaget LM Ericsson, 2014 Annual Report, p. 56; Telefonaktiebolaget LM Ericsson, 2015 Annual Report, p. 56; Telefonaktiebolaget LM Ericsson, 2016 Annual Report, p. 54; Telefonaktiebolaget LM Ericsson, 2017 Annual Report, p. 33; Telefonaktiebolaget LM Ericsson, 2018 Annual Report, p. 45; "Nokia in 2011," Nokia Corporation, 2012, p. 20; Nokia Corporation, Nokia Annual Report on Form 20-F 2012, p. F-2; Nokia Corporation, Nokia Annual Report on Form 20-F 2013, p. F-2; Nokia Corporation, Nokia Annual Report on Form 20-F 2014, p. 142; Nokia Corporation, Nokia Annual Report on Form 20-F 2015, p. 140; Nokia Corporation, Nokia Annual Report on Form 20-F 2016, p. 144; Nokia Corporation, Nokia Annual Report on Form 20-F 2017, p. 148; Nokia Corporation, Nokia Annual Report on Form 20-F 2018, p. 130; Huawei Technologies Co., Ltd., 2010 Annual Report, p. 24; Huawei Technologies Co., Ltd., 2011 Annual Report, p. 32; Huawei Technologies Co., Ltd., 2012 Annual Report, p. 37; Huawei Technologies Co., Ltd., 2013 Annual Report, p. 55; Huawei Technologies Co., Ltd., 2014 Annual Report, p. 60; Huawei Technologies Co., Ltd., 2015 Annual Report, p. 53; Huawei Technologies Co., Ltd., 2016 Annual Report, p. 57; Huawei Technologies Co., Ltd., 2017 Annual Report, p. 64; Huawei Technologies Co., Ltd., 2018 Annual Report, p. 71.

the top 5 of all companies by R&D investment in the world. In comparison, Nokia was ranked 27th and Ericsson was ranked 43rd among all companies by R&D investment in the world.[174]

113. The results of this investment are apparent in Huawei's success in developing 5G technology. For example, Huawei has declared the largest share of 5G standard essential patent families ("SEPs") among all 5G patent owners.[175] According to IPlytics, a company that collects and analyzes patent data and provides tools for patent data analysis,[176] Huawei owned 1,554 5G SEP families as of April 2019. Nokia was the second largest owner after Huawei with 1,427 5G SEP families; Samsung was third with 1,316 5G SEP families; ZTE was fifth with 1,208 5G SEP families; and Ericsson was seventh with 819 5G SEP families.[177]

114. IPlytics also provides statistics on companies' contributions to 5G standards development. Technology standards are developed in international meetings at which companies submit and present technical papers. Huawei is the leader in the number of submitted 5G technical contributions (10,844) to 5G standard development. Ericsson submitted 8,428 contributions; Nokia submitted 5,843 contributions; Samsung submitted 2,621; and ZTE submitted 2,341.[178]

---

[174] Samsung was ranked the top company by R&D investment in the world and the top ICT producer by R&D investment in the world. However, unlike for Huawei, Nokia, and Ericsson, for Samsung, network equipment is not its main line of business. The financial reporting practices by Samsung do not allow me to isolate Samsung's R&D investment in its network equipment business. I have no basis to conclude that Samsung's R&D investment in its network equipment business, and in RAN equipment in particular, is on par with the R&D investment of Huawei, Ericsson, or Nokia. See "EU R&D Scoreboard: The 2018 EU Industrial R&D Investment Scoreboard," *European Commission – Joint Research Centre*, 2018, Table 1.5 and Figure 4.1; Interim Consolidated Financial Statements of Samsung Electronics Co., Ltd. and Its Subsidiaries," Samsung Electronics Company, Ltd., as of March 31, 2019, p. 14; "Earnings Release Q1 2019," Samsung Electronics, April 2019, p. 2.

[175] "Who is leading the 5G patent race? A patent landscape analysis on declared SEPs and standards contributions." *IPlytics*, April 2019 (hereafter, *2019 IPlytics Report*), Table 2, at https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf. SEPs are patented technologies that are designated as necessary for execution of the standard. A vendor manufacturing equipment that complies with the 5G standard, for example, must use the invention claimed by a SEP to comply with the standard.

[176] *2019 IPlytics Report*, p. 7.

[177] *2019 IPlytics Report*, Table 2.

[178] 2019 *IPlytics Report*, Table 5.

115. The attendance of engineers from each company at standards meetings is another measure of how invested the company is in technology development. Huawei is the technology leader by this measure as well, sending far more engineers to the meetings than any other vendor.[179]

116. Additionally, Huawei's commitment to R&D is reflected in its participation in international technical organizations. Huawei is an active member of more than 400 standards organizations, industry alliances, and open source communities.[180]

117. Huawei is also a leader with respect to the number of employees involved in R&D. Huawei reported that in 2018 more than 80,000 employees (45 percent of its total workforce) were involved in R&D.[181] Ericsson reports 24,800 employees (26 percent of its total workforce) working on R&D.[182] Nokia's 2017 "People and Planet" report states that Nokia employed approximately 103,000 people, out of which more than a third (approximately 34,333 employees) worked in R&D.[183]

118. Huawei has received multiple awards for its contributions to 5G technology. Examples of these awards are:

- In 2015, Huawei received the Biggest Contribution to 5G Development award at the 5G World Summit for its contributions relating to research and innovation in 5G technologies.[184]

- At the Mobile World Congress 2017, Huawei received the Outstanding Contribution for LTE Evolution to 5G award, Huawei's Network Function Virtualization ("NFV") solution won the Best Technology Enabler award,

[179] 2019 *IPlytics Report*, pp. 5-6.
[180] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 58.
[181] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 44.
[182] Ericsson Annual Report, 2018, pp. 1, 35.
[183] "People and Planet Report 2017," Nokia Corporation, p. 5.
[184] "Huawei wins award at 5G World Summit 2015," *Daily Observer*, July 3, 2015, at http://www.observerbd.com/2015/07/03/97711.php.

and Huawei's active antenna unit ("AAU") solution won the Best Mobile Infrastructure award.[185]

- In 2017, Huawei's work conducting 5G pre-commercial tests with over 30 leading carriers was recognized as one of the World Leading Internet Scientific and Technological Achievements.[186]

- In June 2017, Huawei received the Best 5G Core Development award at the 5G World Summit held in London.[187]

- In December 2017, "Huawei 3GPP 5G Pre-commercial System," an end-to-end network equipment solution that encompasses RAN and core equipment, was awarded as one of World Leading Internet Scientific and Technological Achievements at the fourth World Internet Conference in Wuzhen, China.[188]

- In 2018, the GSM Association ("GSMA"), an organization that represents the interests of mobile operators and that produces the Mobile World Congress events,[189] awarded Huawei the "Outstanding Contribution to the Mobile Industry Award." This award recognizes individuals, companies, and organizations that have contributed to the advancement of mobile communications in significant ways.[190]

---

[185] Huawei Investment & Holding Co., Ltd., 2017 Annual Report, pp. 24, 26; "Huawei's AAU Solution Awarded Best Mobile Infrastructure at MWC 2017," Huawei, February 28, 2017, at http://carrier.huawei.com/en/Trends-and-insights/AAU-Solution-Awarded-Best-Mobile-Infrastructure?ic_source=fmsh17.

[186] Huawei Investment & Holding Co., Ltd., 2017 Annual Report, p. 24.

[187] Huawei Investment & Holding Co., Ltd., 2017 Annual Report, p. 26.

[188] "Huawei 3GPP 5G Pre-commercial System is awarded as one of World Leading Internet Scientific and Technological Achievement at the Fourth World Internet Conference," Huawei Press Release, December 03, 2017, at https://www.huawei.com/en/press-events/news/2017/12/Huawei-3GPP-5G-Pre-commercial-System.

[189] "About Us," GSM Association, at https://www.gsma.com/aboutus/.

[190] "Huawei Named as Winner of 2018 GSMA Award for Outstanding Contribution to the Mobile Industry," February 26, 2018, GSMA Press Release, at https://www.gsma.com/newsroom/press-release/huawei-named-winner-2018-gsma-award-outstanding-contribution-mobile-industry/.

- In February 2019, Huawei won the "Market Development Award" from the Global TD-LTE Initiative ("GTI")[191] "for its outstanding performance in the 5G commercial market and for its promotion of the end-to-end 5G industry."[192]

B. Huawei's 5G RAN Equipment Is More Highly Ranked Than 5G RAN Equipment of Its Competitors

119. The quality of Huawei's 5G product portfolio has also been demonstrated in head-to-head comparisons. GlobalData, a market research firm headquartered in the United Kingdom,[193] compared 5G mobile base station portfolios offered by Huawei, Ericsson, Nokia, Samsung, and ZTE[194] on the following four criteria: (1) baseband unit capacity, (2) breadth of radio unit portfolio, (3) ease of installation, and (4) technology evolution. GlobalData found Huawei's 5G RAN equipment to lead in every category.[195]

120. A recent study by RootMetrics[196] also documents the quality of Huawei's equipment. RootMetrics tested performance of 5G networks deployed by major carriers KT, LG Uplus, and SK Telecom in South Korea in the high-population areas in Seoul and in suburban areas around Seoul. The 5G networks were tested between June 28, 2019 and July 6, 2019.[197]

---

[191] GTI is the global initiative that advocates cooperation among carriers to promote LTE-TDD. "Global TD-LTE Initiative (GTI) Announced to Promote the Deployment of TD-LTE Networks," *PRNewswire-Asia*, February 14, 2011, at https://www.prnewswire.com/news-releases/global-td-lte-initiative-gti-announced-to-promote-the-deployment-of-td-lte-networks-116176069.html.

[192] "Huawei Wins 'Market Development Award' from GTI for its Outstanding Performance in 5G Commercialization," Huawei Press Release, February 22, 2019, at https://www.huawei.com/us/press-events/news/2019/2/huawei-wins-market-development-award-from-gti.

[193] "Why GlobalData," GlobalData, at https://www.globaldata.com/who-we-are/why-globaldata/.

[194] "Telecom industry's first 5G RAN competitive analysis published by GlobalData reveals Huawei leadership," GlobalData Press Release, July 25, 2019, at https://www.globaldata.com/telecom-industrys-first-5g-ran-competitive-analysis-published-by-globaldata-reveals-huawei-leadership/.

[195] "Telecom industry's first 5G RAN competitive analysis published by GlobalData reveals Huawei leadership," GlobalData Press Release, July 25, 2019, at https://www.globaldata.com/telecom-industrys-first-5g-ran-competitive-analysis-published-by-globaldata-reveals-huawei-leadership/.

[196] RootMetrics is a mobile analytics firm that provides insights into the user experience of mobile networks. "Providing insights to help improve the end-user mobile experience," RootMetrics by IHS Markit, at http://rootmetrics.com/en-US/about.

[197] "5G First Look South Korea," RootMetrics by IHS Markit, at http://rootmetrics.com/en-US/content/5g-first-look-south-korea-US.

121. RootMetrics reported the results for download speeds, availability, reliability, and latency.[198] The study found that all three carriers had excellent reliability for getting connected and staying connected to 5G networks.[199] It also found that LG Uplus delivered the fastest median and maximum 5G download speeds, had the most consistent speed performance, and had the lowest median download latency among all tested networks.[200]

122. It is reported that 90 percent of LG Uplus's network in the tested areas uses Huawei 5G equipment including Huawei 5G Massive MIMO equipment, which I will discuss in the next section.[201] Neither KT nor SK Telecom uses Huawei equipment in their 5G networks. KT and SK Telecom use 5G RAN supplied by Samsung, Ericsson, and Nokia.[202] These results are consistent with Huawei's leading position in 5G RAN.

123. As these facts and results show, Huawei is a global R&D leader in 5G RAN. Huawei invests heavily in R&D, both monetarily and in human resources, and its investment bears results in creating expertise that is memorialized in the quality and efficiency of its products.

C. Huawei's Massive MIMO Equipment Is in Far Greater Demand Than That Available from Any Other Vendor

124. One of the key components of 5G RAN is known as "Massive MIMO." Massive MIMO (multiple input, multiple output[203]) is antenna technology that deploys a large number of

---

[198] Reliability shows the frequency of download failures when attempting to access 5G network and the frequency of download failures after connecting to 5G network. See "5G First Look South Korea," RootMetrics by IHS Markit, at http://rootmetrics.com/en-US/content/5g-first-look-south-korea-US.

[199] RootMetrics graded download reliability as "excellent" if successful download was achieved at a rate of 97 percent. See "5G First Look South Korea," RootMetrics by IHS Markit, at http://rootmetrics.com/en-US/content/5g-first-look-south-korea-US.

[200] "5G First Look South Korea," RootMetrics by IHS Markit, at http://rootmetrics.com/en-US/content/5g-first-look-south-korea-US.

[201] See "South Korea's 5G Network Test Announcement: Huawei Definitely Boosts LG U+ to Come out Ahead," C114, August 13, 2019 (translated from Chinese), at http://www.c114.com.cn/news/126/a1097014.html.

[202] Iain Morris, "Samsung Pumps Up the Basestations [*sic*] in Korean 5G Market," *LightReading*, April 11, 2019, at https://www.lightreading.com/mobile/5g/samsung-pumps-up-the-basestations-in-korean-5g-market/d/d-id/750772.

[203] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, p. 11.

two-dimensional arrays of active antennas at the base station.[204] Massive MIMO technology is an evolution of MIMO antenna technology;[205] Massive MIMO antennas generally have at least 32 antennas at the base station.[206] MIMO systems increase signal strength and deliver focused beams that can track user handsets and user equipment.[207] The large number of focused antenna elements allow the base station to concentrate its energy where it is needed, thereby reducing interference and achieving a much higher network capacity and better coverage.[208]

125. MIMO antennas were developed for and used in 4G wireless networks.[209] Massive MIMO antenna systems have also been used in LTE networks to improve capacity and coverage,[210] and this technology is expected to be a critical component of 5G deployment.[211] According to some reports, adequate 5G performance requires Massive MIMO to have a minimum of 64 antennas, and up to 256.[212] Massive MIMO is anticipated to be used in mid-band and mmW spectrum bands,[213] but not in low spectrum bands, because the longer wavelengths

---

[204] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, p. 4.

[205] Thomas L. Marzetta, *et al*., FUNDAMENTALS OF MASSIVE MIMO, Cambridge: Cambridge University Press, 2016, p. 5.

[206] Matti Passoja, "5G NR: Massive MIMO and Beamforming – What does it mean and how can I measure it in the field?," RCRWireless, September 12, 2018, https://www.rcrwireless.com/20180912/5g/5g-nr-massive-mimo-and-beamforming-what-does-it-mean-and-how-can-i-measure-it-in-the-field; "A closer look at Massive MIMO," Sprint Business, November 7, 2018, at https://business.sprint.com/blog/massive-mimo/.

[207] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, p. 20.

[208] Edison Lee and Timothy Chau, "Telecom Services: The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, p. 20.

[209] "4x4 MIMO Boosts 4G and Gives Consumers a Taste of the Gigabit Experience," *Strategy Analytics*, November 2017, p. 4.

[210] "4x4 MIMO Boosts 4G and Gives Consumers a Taste of the Gigabit Experience," *Strategy Analytics*, November 2017, p. 16-17.

[211] "4x4 MIMO Boosts 4G and Gives Consumers a Taste of the Gigabit Experience," *Strategy Analytics*, November 2017, p. 18.

[212] Edison Lee and Timothy Chau, "Telecom Services. The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, p. 20.

[213] Narcis Cardona, Luis M. Correia, Daniel Calabuig, "Key Enabling Technologies for 5G: Millimeter-Wave and Massive MIMO," *International Journal of Wireless Information Networks* 24, iss. 3 (September 2017), pp. 201-202.

of the lower spectrum bands require antennas that are too large to be accommodated by Massive MIMO.[214]

126. Dell'Oro Group's data show that that Massive MIMO has accounted and will account for the vast majority of total 5G RAN spending over Q4 2018-Q1 2020. Sales of Massive MIMO are projected by analyst Dell'Oro Group to comprise an overwhelming majority of total 5G RAN spending in the last three quarters of 2019, before declining in 2020.

127. The evidence suggests that Huawei has the most advanced Massive MIMO products available today. Multiple sources, including the U.S. Department of Defense, conclude that Chinese equipment manufacturers, and Huawei in particular, have been leaders in Massive MIMO technology.[215]

128. A report by ABI Research, a New-York-based industry research firm,[216] compared and ranked "the ten most dominant and innovative mobile cellular antenna manufacturers in the world."[217] These included ACE Technologies, Amphenol, Comba, CommScope, Huawei, Kathrein, MOBI, RFS, Rosenberger, and Tongyu.[218] ABI Research analyzed the following characteristics of each vendor: "multi-band, ultra-wideband, active, and advanced MIMO capabilities, essential intellectual property and R&D, overall market

---

[214] "Professor Rappaport Explains Why T-Mobile 5G 600 MHz Ultimately Doesn't Make It," Wireless One, May 3, 2018, at http://wirelessone.news/10-r/1037-professor-rappaport-explains-why-t-mobile-5g-600-mhz-are-a-dud.

[215] A report from the Defense Innovation Board called Huawei and ZTE "the leader [*sic*] in massive MIMO radio systems." See Milo Medin and Gilman Louie, "The 5G Ecosystem: Risks & Opportunities for DoD," Defense Innovation Board, April 2019, p. 17; Rethink Technology Research said that "Huawei has been in front of the field in areas such as Massive MIMO and flexible spectrum usage." See Caroline Gabriel, "Nokia and Ericsson pin hopes on 5G to catch up with Huawei," *Riot*, August 2018, at https://rethinkresearch.biz/articles/nokia-and-ericsson-pin-hopes-on-5g-to-catch-up-with-huawei-2/. According to the Wall Street Journal, European carriers said that Nokia and Ericsson "have been slow to release equipment as advanced as Huawei's." See "Huawei's dominance in 5G technology makes it nearly impossible to restrict the controversial Chinese company from telecom networks," *Wall Street Journal*, video at 2:24, at https://www.wsj.com/video/why-it-almost-impossible-to-extract-huawei-from-telecom-networks/122E816F-856B-4D3F-A361-B832D9862A99.html.

[216] "About Us: Who We Are," ABI Research, at https://www.abiresearch.com/pages/about-abi-research/; "Office Locations," ABI Research, at https://www.abiresearch.com/contact/.

[217] "Huawei and Kathrein Ranked Top Two Base Station Antenna Vendors in New ABI Research Competitive Assessment," ABI Research press release, August 8, 2019, at https://www.abiresearch.com/press/huawei-and-kathrein-ranked-top-two-base-station-antenna-vendors-new-abi-research-competitive-assessment/.

[218] "Huawei and Kathrein Ranked Top Two Base Station Antenna Vendors in New ABI Research Competitive Assessment," ABI Research press release, August 8, 2019, at https://www.abiresearch.com/press/huawei-and-kathrein-ranked-top-two-base-station-antenna-vendors-new-abi-research-competitive-assessment/.

share, antenna geographical penetration, financial and organizational health, and antenna portfolio."[219]

129. ABI Research ranked Huawei as the top vendor in innovation and implementation, followed by Kathrein (which is in the process of being acquired by Ericsson[220]) in the second place and CommScope in the third place. ABI Research reported that in 2018 Huawei was the largest antenna manufacturer in the market, and its market share (34.4 percent) was almost double the market share of its nearest competitor Kathrein (19.6 percent).[221]

130. Huawei's leadership in Massive MIMO technology may be the result of two factors in addition to Huawei's overall R&D leadership documented earlier.

131. First, Massive MIMO technology emerged from LTE-TDD,[222] a technology in which Huawei has unusually extensive expertise, as I explain below. There are two common technologies through which radio communications systems can communicate in both directions (i.e., to transmit and to receive a signal): TDD and FDD. The TDD method uses the same frequency channel to transmit and receive signals from a given handset or device but allocates different time slots for transmission and reception.[223] FDD uses different frequency channels, one for transmission and one for reception.[224]

---

[219] "Huawei and Kathrein Ranked Top Two Base Station Antenna Vendors in New ABI Research Competitive Assessment," ABI Research press release, August 8, 2019, at https://www.abiresearch.com/press/huawei-and-kathrein-ranked-top-two-base-station-antenna-vendors-new-abi-research-competitive-assessment/.

[220] According to news articles, this acquisition is expected to close in the third quarter of 2019. See "Ericsson buys antenna and filters business of Germany's Kathrein," *Reuters*, February 25, 2019, at https://www.reuters.com/article/us-kathrein-m-a-ericsson-idUSKCN1QE0SF.

[221] "Huawei and Kathrein Ranked Top Two Base Station Antenna Vendors in New ABI Research Competitive Assessment," ABI Research press release, August 8, 2019, at https://www.abiresearch.com/press/huawei-and-kathrein-ranked-top-two-base-station-antenna-vendors-new-abi-research-competitive-assessment/; "Huawei's innovation capability continues to lead, and the global passive antenna market share reaches 34.4%," C114, August 30, 2019 (translated from Chinese), at http://www.c114.com.cn/news/126/a1099418.html.

[222] Daryl Schoolar, "Massive MIMO Comes of Age," Ovum, 2017, p. 3.

[223] "LTE FDD, TDD, TD-LTE Duplex Schemes," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/4g-lte-long-term-evolution/tdd-fdd-td-lte-duplex-schemes.php.

[224] "LTE FDD, TDD, TD-LTE Duplex Schemes," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/4g-lte-long-term-evolution/tdd-fdd-td-lte-duplex-schemes.php.

132. Although there is an FDD version of Massive MIMO, I understand that the majority of Massive MIMO currently deployed uses TDD technology.[225] This is because Massive MIMO achieves spectrum efficiency by directing its beams to specific locations where it detects devices, a process called "beamforming."[226] From a lay perspective, because TDD uses only one frequency channel to both transmit and receive while FDD uses separate frequency channels for transmission and reception, the real-time calculations necessary to identify and direct the beams to and from mobile devices need only be done (at each point in time) once under TDD rather than twice, a material saving in complexity.[227] TDD Massive MIMO is more widespread than FDD Massive MIMO due to these properties of the TDD technology that simplify the algorithm for the beamforming technology.[228]

133. Few carriers in the world operate LTE-TDD networks; LTE-FDD is by far the more commonly deployed 4G technology.[229] Huawei, however, has extensive LTE-TDD expertise because TD-SCDMA evolved into LTE-TDD, and TD-SCDMA, as noted earlier, was developed in China and adopted by the largest[230] Chinese carrier, China Mobile.[231] Currently, China Mobile is the largest LTE-TDD carrier in the world,[232] and Huawei is one

[225] Daryl Schoolar, "Massive MIMO Comes of Age," Ovum, 2017, p. 3.

[226] "Massive MIMO," Sprint, at https://business.sprint.com/5g/massive-mimo/.

[227] "A closer look at Massive MIMO," Sprint Business, November 7, 2018, at https://business.sprint.com/blog/massive-mimo/.

[228] Daryl Schoolar, "Massive MIMO Comes of Age," Ovum, 2017, p. 3.

[229] LTE TDD is also called TD-LTE. See "LTE FDD, TDD, TD-LTE Duplex Schemes," *Electronics Notes*, at https://www.electronics-notes.com/articles/connectivity/4g-lte-long-term-evolution/tdd-fdd-td-lte-duplex-schemes.php; "GSA confirms 521 LTE networks launched, LTE-Advanced now mainstream," Global mobile Supplier Association, August 12, 2016, at https://gsacom.com/press-release/gsa-confirms-521-lte-networks-launched-lte-advanced-now-mainstream/.

[230] Approximately 60 percent of mobile connections in China were through China Mobile in Q4 2018. 925,069,000/1,543,105,000 = 59.9 percent. See GSMA Intelligence 2019 subscriber data for China.

[231] Pete Bell, "4G Breaks Through That Great Chinese Wall," *TeleGeography*, August 24, 2016, at https://blog.telegeography.com/4g-market-in-china-subscriber-growth-of-china-mobile.

[232] Edison Lee and Timothy Chau, "Telecom Services. The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, September 14, 2017, p. 9.

of the suppliers of LTE equipment to China Mobile.[233] As a result, Huawei had the largest revenue share of sales of LTE-TDD equipment among all vendors between 2011 (when the sales of LTE-TDD equipment started)[234] and 2018.[235]

134. Huawei's deep experience in LTE-TDD has allowed Huawei to leverage its TDD expertise into Massive MIMO antenna technology.

135. Huawei's leadership in Massive MIMO technology shows in Huawei's revenue share in sales of Massive MIMO equipment used in LTE networks. Dell'Oro data indicates that Huawei is by far the largest supplier of Massive MIMO for LTE. Its revenue share in 2018 exceeded that of the next largest supplier by a factor of over 9.[236]

136. Huawei has also been a leader in sales of Massive MIMO used in 5G deployments. Data on the early deployments of 5G show that Huawei and Samsung were the largest suppliers of 5G Massive MIMO in Q4 2018 and in Q1 2019.[237]

137. The surprising increase in Samsung's share of Massive MIMO sales for 5G relative to LTE is likely reflective of the facts that, as noted earlier, South Korea was one of the major deployers of 5G during the time period covered by the data and that Samsung has a substantial share of equipment sales in South Korea, its home country. Ericsson was able to more than double its revenue share from 2018 to Q1 2019, likely due to its partnership with Sprint, which was using Massive MIMO to roll out its 5G network in the United

---

[233] In 2011, Huawei named China Mobile as one of its "key customers." See Huawei Investment & Holding Co., Ltd., 2011 Annual Report, p. 93, at https://www.huawei.com/ucmf/groups/public/documents/attachments/hw_126991.pdf. In 2013, Huawei stated that it is a "strategic partner" of China Mobile. See Huawei Investment & Holding Co., Ltd., 2013 Annual Report, p. 29, at https://www.huawei.com/ucmf/groups/public/documents/attachments/hw_u_323372.pdf. In 2014, Huawei stated that it had become "the most important strategic partner of China Mobile...in the area of LTE construction." See Huawei Investment & Holding Co., Ltd., 2014 Annual Report, p. 22, at https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annualreport2014_en.pdf?la=en-us. Huawei helped China Mobile to deploy the world's largest VoLTE network. See Huawei Investment & Holding Co., Ltd., 2016 Annual Report, p. 23, at https://www-file.huawei.com/-/media/CORPORATE/PDF/annual-report/AnnualReport2016_en.pdf?la=en; Huawei Investment & Holding Co., Ltd., 2017, p. 26, at https://www-file.huawei.com/-/media/corporate/pdf/annual-report/annual_report2017_en.pdf?la=en.

[234] "MOBILE RADIO ACCESS NETWORK – LTE – FDD," Dell'Oro Group, Q1 2019.

[235] Based on data provided by Dell'Oro Group.

[236] Based on data provided by Dell'Oro Group.

[237] Based on data provided by Dell'Oro Group.

States.[238] Huawei's substantial revenue shares were achieved despite having no sales of 5G Massive MIMO in the United States.

VIII. CONTINUING TO LIMIT HUAWEI'S PARTICIPATION IN THE U.S. MARKET WILL DELAY THE U.S. TRANSITION TO 5G

138. Continuing to exclude Huawei from the U.S. market will impede U.S. deployment of 5G and harm the U.S. economy.

A. Early Deployment of New Wireless Technology Benefits a Country

139. Leadership in a new generation of wireless technology benefits a country. Recon Analytics, a market research firm focusing on the telecommunications industry,[239] defines leadership in each generation of wireless technology as the status of being among the first to deploy a working network and being among the first to reach material levels of penetration and adoption of the technology.[240] Recon Analytics argues that the benefits of such leadership include "the strong economic contributions of wireless manufacturers to their balance of trade, the employment of hundreds of thousands, and the generation of intellectual capital and property rights."[241]

140. Deloitte has found that the global leaders in previous generations of wireless networks were rewarded greater macroeconomic benefits than non-leading countries.[242] Deloitte predicts that being a leader in 5G will generate even more benefits than did leadership in earlier technologies due to positive network effects associated with the billions of devices that will connect to 5G networks.[243] Deloitte argues that as more devices connect to 5G networks, companies will be able to collect and analyze data in order to provide more valuable

---

[238] "Sprint Lights Up True Mobile 5G in Atlanta, Dallas-Fort Worth, Houston and Kansas City," Sprint Press Release, May 30, 2019, at https://newsroom.sprint.com/sprint-lights-up-true-mobile-5g-in-atlanta-dallas-fort-worth-houston-and-kansas-city.htm.

[239] "About Us," *Recon Analytics*, at http://reconanalytics.com/about-us/.

[240] *Recon Analytics Report 2018*, p. 3.

[241] *Recon Analytics Report 2018*, p. 4.

[242] "5G: The chance to lead for a decade," Deloitte, 2018, p. 2.

[243] In economics, a network effect occurs when the value of a product or service depends on the number of users. "5G: The chance to lead for a decade," Deloitte, 2018, p. 2.

services.[244] As a result, "countries that adopt 5G first are expected to experience disproportionate gains in macroeconomic impact compared to those that lag."[245]

B. Impacts of Wireless Telecommunications Technology on Economic Growth and Productivity

141. Economic analysis demonstrates that telecommunications technology boosts GDP. Indeed, the relationship between mobile broadband technology (and the telecommunications industry in general) and economic growth has been studied by economists for several decades.

142. There are a number of channels through which mobile telecommunications contribute to GDP.

143. First, deployment of mobile infrastructure directly benefits the economy through expenditures made by carriers and through jobs generated during infrastructure deployment. I refer to these contributions to GDP as "direct" effects.

144. Second, there are also "indirect" effects that are significant for telecommunications technologies, because telecommunications technologies enable innovation and productivity gains in many other sectors throughout the economy.[246] For example, as elaborated earlier, telecommunications enable services ranging from traditional telephony to video calls, mobile banking, video streaming, online games, tele-working,[247] GPS-based services, e-commerce, and transportation services, among many others. Modern telecommunications technology enables users to collaborate and exchange information over long distances and access and exchange data while they travel. Innovation enabled by new telecommunications technology leads to the production of new applications and devices, creation of companies, and improvements in ways of working, living, and

---

[244] "5G: The chance to lead for a decade," Deloitte, 2018, p. 2.

[245] "5G: The chance to lead for a decade," Deloitte, 2018, p. 2.

[246] Harald Gruber and Pantelis Koutroumpis, "Mobile telecommunications and the impact on economic development," *Economic Policy* (July 2011) (hereafter, *Gruber and Koutroumpis (2011)*), p. 390, at https://www.jstor.org/stable/41261993?seq=1#metadata_info_tab_contents; Timothy F. Bresnahan and Manuel Trajtenberg, "General purpose technologies 'Engines of growth'?" *Journal of Econometrics* 65, no. 1 (1995), p. 84.

[247] *Gruber and Koutroumpis (2011)*, p. 392.

learning.[248] These innovative services and goods improve productivity and contribute to the overall growth of the economy.[249]

145. The development of the 5G ecosystem and of the extensive array of new services and industries arising from 5G will all amplify GDP growth. 5G is anticipated to enable innovation in transport, logistics, IoT, electricity distribution, public safety, health and wellness, and smart cities.[250] An Accenture study on 5G deployment predicts that, between direct and indirect effects, the rollout of 5G could create up to 3 million additional jobs and annually boost GDP by $500 billion in the United States.[251]

146. The indirect effects of telecommunications technology, such as the production of new applications and devices, become more pronounced as more individuals use the technology.[252] Several economic studies have estimated the effect of availability and penetration of a mobile technology on GDP.

147. Economists Robert Crandall and Charles Jackson evaluated the impact on the U.S. economy of faster roll-out of broadband access, including both wireless and landline. They concluded that the benefits are substantial:

> [A] reasonable figure for the total annual benefits to the U.S. economy of the widespread adoption of broadband access in all its forms—ADSL, cable modems, satellites, 3G wireless, and others—could be more than 400 billion dollars per year. Faster rollout of high-speed access services gives us these benefits

---

[248] "The impact of 4G technology on commercial interactions, economic growth, and U.S. competitiveness," Deloitte, August 2011, p. 2.

[249] *Gruber and Koutroumpis (2011)*, p. 392.

[250] See 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Release 15 Description; Summary of Rel-15 Work Items (Release 15), TR 21.915 v1.0.0 (2019-03), pp. 9-10.

[251] "Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities," *Accenture Strategy*, 2017, at https://www.accenture.com/t20170222T202102__w__/us-en/_acnmedia/PDF-43/Accenture-5G-Municipalities-Become-Smart-Cities.pdf, p. 3. Accenture estimates the *overall* effect that 5G deployment and penetration will have on GDP and employment over seven years. In my report in Section VIII.E, I estimate the effect of *delay* in 5G deployment and penetration on GDP and employment over the 2019-2024 period. Because I estimate the effect on employment using a multiplier approach discussed in detail in Section VIII.E.iv, the delay in 5G deployment affects employment only in years 2019 and 2020 (as I explain in Section VII.E.iv, after 2020 the investment in 5G catches up with what the investment would have been without a delay in 5G deployment). Due to these differences, the effects on GDP and employment that I estimate in Section VIII.E are substantially lower than the effects on GDP and employment estimated by Accenture.

[252] *Gruber and Koutroumpis (2011)*, p. 390.

> earlier. A reasonable estimate of the net present value of faster rollout of broadband is as much as 500 billion dollars. Under the more modest scenario of 50 percent adoption, the net present value of faster rollout would be about 140 billion dollars.[253]

148. Economists Harald Gruber and Pantelis Koutroumpis, using panel data from 192 countries over the 1990-2007 period, found that an increased number of mobile lines, which is their proxy for the diffusion of mobile telecommunications,[254] results in higher GDP growth.[255] Economist Harald Edquist and coauthors, using data for 90 countries over the 2002-2014 period, found that a 10 percent increase in mobile broadband adoption increases GDP by 0.8 percent.[256]

149. A study by Deloitte examined the impact of the penetration of a new generation of wireless technology on GDP, using data from the transition from 2G to 3G. The study examined a panel of 96 developed and developing countries over the 2008-2011 period to estimate the impact of the penetration rate of new 3G technology in a country on its GDP per capita. It found that a 10 percent increase in the 3G penetration rate increased GDP per capita by 0.15 percent.[257]

150. Just as increased technology penetration increases GDP, delays in technology penetration will dampen GDP growth. Economist Jerry Hausman estimated the losses to consumer welfare in the United States due to the delay in the introduction (and, therefore, in the availability and penetration) of cellular service in the United States, which was result of the FCC's regulatory indecision. Using price and subscribership data for the 1989-1993 period from a confidential survey of cellular carriers, Hausman estimated that annual consumer welfare loss ranged from $16.7 billion to $33.5 billion in 1994 dollars, which is

---

[253] See Robert Crandall and Charles Jackson, "The $500 Billion Opportunity," in DOWN TO THE WIRE: STUDIES IN THE DIFFUSION AND REGULATION OF TELECOMMUNICATIONS TECHNOLOGIES, ed. Allan Shampine (Nova Science Publishers, 2003), p. iv.

[254] *Gruber and Koutroumpis (2011)*, p. 396.

[255] *Gruber and Koutroumpis (2011)*, pp. 400-402, Table 2.

[256] Harald Edquist *et al.*, "How important are mobile broadband networks for the global economic development?" *Information Economics and Policy* 45 (2018), pp. 17, 19, Table 7.

[257] "What is the impact of mobile telephony on economic growth? A Report for the GSM Association." *Deloitte*, November 2012, pp. 2, 11, 13-14.

equivalent to welfare losses of $28.7 billion to $57.6 billion in 2019 dollars.[258] He also found that this regulatory indecision delayed the provision of cellular services by seven to ten years in the U.S., which in total translated into welfare losses ranging from $116.9 billion to $335 billion in 1994 dollars, which is equivalent to welfare losses of $200.9 billion to $575.7 billion in 2019 dollars.[259]

C. Continued Exclusion of Huawei Will Further Delay 5G Deployment and Penetration

151. As already noted, the evidence from data on 5G RAN equipment spending indicates that the United States is behind in 5G deployment. The most recently available data show that spending on 5G RAN equipment in North America is on the order of a third of that in Asia Pacific.[260]

152. The slow start of the United States in 5G deployment is undoubtedly due at least in part to the spectrum gap that I discussed earlier. It may not be possible for the United States to catch up to those countries that have already been deploying commercial 5G networks on a wide scale even once the FCC allocates mid-band spectrum for 5G use. History shows that countries that lag in initial penetration of a new technology tend to continue to lag behind for several years in that technology. Figure VIII.1 shows the 4G penetration rate

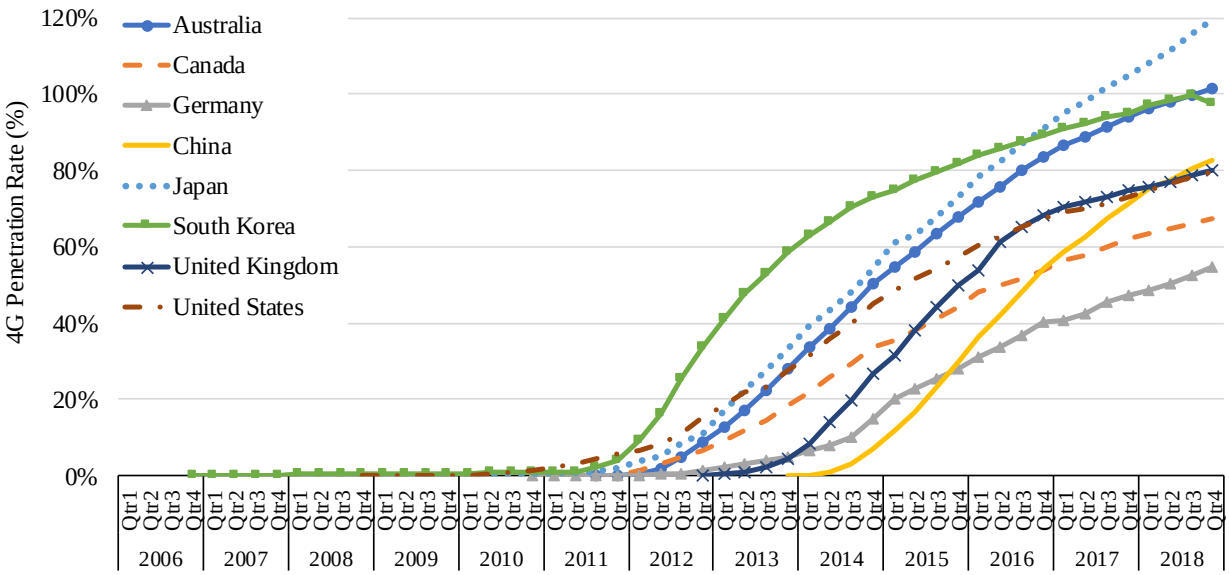
[258] Jerry Hausman, "Valuing the Effects if Regulation on New Services in Telecommunications," *Brookings Papers: Microeconomics* (1997), pp. 20, 23. I converted losses expressed in 1994 dollars into 2019 dollars by multiplying losses in 1994 by the ratio of CPI in 2019 to CPI in 1994. CPI for 1994 is calculated as the average of monthly CPIs in 1994. CPI for 2019 is calculated as the average of monthly CPIs from January 2019 through July 2019. See "Historical Consumer Price Index for All Urban Consumers (CPI-U): U.S. city average, all items, by month," Bureau of Labor Statistics, July 2019, at https://www.bls.gov/cpi/tables/supplemental-files/historical-cpi-u-201907.pdf.

[259] Jerry Hausman, "Valuing the Effects if Regulation on New Services in Telecommunications," *Brookings Papers: Microeconomics* (1997), pp. 20, 23. I converted losses expressed in 1994 dollars into 2019 dollars by multiplying losses in 1994 by the ratio of CPI in 2019 to CPI in 1994. CPI for 1994 is calculated as the average of monthly CPIs in 1994. CPI for 2019 is calculated as the average of monthly CPIs from January 2019 through July 2019. See "Historical Consumer Price Index for All Urban Consumers (CPI-U): U.S. city average, all items, by month," Bureau of Labor Statistics, July 2019, at https://www.bls.gov/cpi/tables/supplemental-files/historical-cpi-u-201907.pdf.

[260] See Section V.

over time for eight countries for which data are available to me. As the figure shows, many countries that start out behind tend to stay behind.[261]

Figure VIII.1
4G Penetration Rate - Selected Countries, Q1 2006 - Q4 2018



Source: GSMA Intelligence, "Country Dashboard," 2019, for Australia, Canada, China, Germany, Japan, South Korea, the United Kingdom, and the United States.

153. Because the United States is already delayed relative to other leading countries, the ability of the United States to become a leading country in 5G deployment and penetration will depend on its ability to recover quickly from its initial slow start. Recovering quickly will require, in turn, access to the best available equipment and fostering of the most competitive equipment market. The absence of Huawei—the market technology leader in 5G RAN technologies generally and in Massive MIMO technology in particular—will

[261] Using the data underlying this figure, I identified 27 country pairs, in which one country (the "follower country") launched 4G after the other country (the "leader country"). For example, in the country pair South Korea-Australia, South Korea is the leader country (it launched 4G in Q4 2006) and Australia is the follower country (it launched 4G in Q3 2011). Out of 27 country pairs, only 13 follower countries caught up with the leader countries. I consider that a follower country catches up with a leader country if its 4G penetration rate stays consistently equal to or above the 4G penetration rate of the leader country. I did not include country pair Australia-Canada in this analysis because Australia and Canada launched 4G networks in the same quarter.

inevitably damage the ability of the United States to regain lost ground to the extent it is possible.

154. There are several reasons that the continued absence of Huawei from the U.S. market will not only damage the ability of the United States to recover from its slow start in 5G deployment but will further delay it.

i. Huawei's RAN Equipment, Especially Massive MIMO, Is Among the Most Widely Used in the World, Thus Implying a More Developed Ecosystem that Facilitates Deployment and Adoption

155. As I discussed in Section VII, Huawei's RAN equipment, especially Massive MIMO, is among the most widely used globally. As more carriers adopt a particular technology its installation and use drive additional knowledge and foster the development of related equipment. Improved knowledge and a broader equipment portfolio in turn enhance the ease of installation and use of new networks, further accelerating deployment.

ii. Huawei's Competitive Presence Would Drive Down Prices of Other Vendors' RAN Equipment, Thus Encouraging Faster Deployment of 5G

156. The market for RAN equipment is highly concentrated in the United States. As I have discussed, there are only five RAN equipment vendors with the R&D muscle and capabilities to provide 5G RAN equipment in the world today, and only two of these have a substantial revenue share in the United States. The fact that the market for 5G RAN equipment is so highly concentrated in the United States inevitably causes equipment prices to be higher than they would be with additional competition from Huawei, the largest vendor of RAN equipment in the rest of the world today.[262] I will discuss this conclusion in greater detail in Section IX.

157. Correspondingly, permitting Huawei to sell in the United States would increase competition among equipment vendors for carriers' business and would be expected to

[262] Based on the data provided by Dell'Oro Group.

drive equipment prices down. The reduction in equipment prices would, in turn, allow carriers to deploy 5G networks more quickly for a given volume of capital expenditures.

iii. Simultaneous Deployment of 5G Around the World Imposes Pressure on the Global Supply Chain of RAN Equipment, Leading to Delays

158. As I have discussed in Section V.B.ii, carriers around the world are simultaneously deploying 5G networks, and many seek to be leaders in 5G deployment. Many countries are preparing to start rolling out 5G networks in addition to those already deploying 5G networks. To the extent that Ericsson, Nokia, and Samsung, the main suppliers of 5G RAN in the United States, have already made commitments to carriers in other countries to supply equipment, their ability to supply U.S. carriers may be limited in the short run. Indeed, as noted earlier, Nokia, one of the major U.S. suppliers, has already experienced delays in supplying equipment to South Korea.[263]

iv. Huawei's 5G RAN Equipment Is the Most Advanced in the World, and Its Absence Will Affect the Quality of Services Available to U.S. Mobile Wireless Customers, Thereby Depressing Customer Acceptance

159. As documented earlier, the data on acceptance of Huawei equipment as measured by both its revenue shares and its independent quality ratings indicate that Huawei sells the leading 5G equipment in the world today. As also documented, countries that use Huawei equipment in their 4G networks have on average far superior network performance than do U.S. networks. Even if U.S. carriers were able to deploy 5G networks equally quickly with or without Huawei in the marketplace, the evidence is that the quality of these networks would be inferior to their performance if Huawei 5G RAN equipment were included.

160. Penetration of a new technology depends not only on the availability of the network, but also on the benefits it provides over and above existing services to which customers have become accustomed. This is because adoption of a new technology, especially for early adopters, requires upgraded handsets.[264] Hence, the speed with which a significant number

[263] See Section VI.
[264] See Appendix D for examples of 5G-capable handsets.

of customers will transition to a new technology will be accelerated when the benefits of the new service are more attractive or otherwise more apparent to users. The speed with which penetration of 5G grows in the United States will, accordingly, be dampened from its starting point by exclusion of what is currently known as the leading equipment in the world.

D. Other Observers Have Also Concluded that Exclusion of Huawei Will Cause Delay in 5G Network Deployment

161. A study by U.K.-based analyst firm Assembly analyzed the impact of a partial or complete restriction on Huawei in the U.K. market for RAN equipment on carriers' 5G rollout timeline. In the course of this study, Assembly interviewed three out of the four major U.K. carriers.[265] Assembly found that the exclusion of Huawei from the United Kingdom would delay deployment there by 18 to 24 months, of which 9 to 18 months would be needed for Huawei's competitors to bridge the technological gap. The study also found that, depending on the severity of restriction, additional time might be required to replace Huawei's equipment in the existing networks.[266]

162. Policy makers and carriers have also concluded that placing restrictions on Huawei would result in significant delays in 5G deployment. For example, Telus Corp., a Canadian provider of wireless telecommunications services, has warned of potential delays in 5G deployment and added costs if Huawei's 5G network equipment is banned from the Canadian market.[267] The Wall Street Journal reported that according to some senior executives of wireless carriers, Huawei's 5G technology may be up to one year ahead of

---

[265] "The Impact on the UK of a Restriction on Huawei in the Telecoms Supply Chain," Assembly, April 5, 2019, pp. 3, 6, 8-10, at http://www.mobileuk.org/The%20impact%20on%20the%20UK%20of%20a%20restriction%20on%20Huawei%20in%20the%20telecoms%20supply%20chain.pdf.

[266] "The Impact on the UK of a Restriction on Huawei in the Telecoms Supply Chain," Assembly, April 5, 2019, pp. 3, 8-10, at http://www.mobileuk.org/The%20impact%20on%20the%20UK%20of%20a%20restriction%20on%20Huawei%20in%20the%20telecoms%20supply%20chain.pdf.

[267] Natalie Wong, "Telus Warns of Potential Cost Fallout if Canada Bans Huawei," *Bloomberg*, February 14, 2019, at https://www.bloomberg.com/news/articles/2019-02-14/telus-says-huawei-ban-could-materially-raise-5g-deployment-cost.

its Western rivals.[268] A study by GSMA found that banning telecom equipment from Huawei and ZTE in Europe would delay deployment of 5G networks by about 18 months due to delivery challenges by vendors such as Nokia, Ericsson, and Samsung.[269] The chief technology officer of BT Group plc ("BT")—a U.K.-based communications services company that offers its services in 180 countries[270]—Howard Watson said at an industry event in March 2019 that Huawei's 5G technology was 18 months ahead of Ericsson's and Nokia's 5G technology.[271] BT's chief architect Neil McRae stated that "there is only one true 5G supplier right now and that is Huawei—the others need to catch up." He did not specify the extent of the technological gap between Huawei and its competitors.[272] In February 2019, a senior technology analyst at the research firm Fitch Solutions reported that based on his conversations with carriers Huawei is "far more advanced than the other two [Ericsson and Nokia] right now."[273]

E. The Economic Impact of the Delay of 5G Deployment on the U.S. Economy, Incorporating the Effects of Depressed Penetration

163. When a new technology is expected to generate considerable benefits for the economy, delaying or impeding the development of the infrastructure for that technology will lead to delayed penetration of the technology (i.e., delayed adoption of the technology by consumers and businesses), which will in turn inevitably generate substantial losses to the economy. I have applied econometric and economic techniques to quantify the effect on the U.S. economy of the incremental delay caused by Huawei's exclusion.

---

[268] Wall Street Journal video, Sarah Krouse, "Huawei Presses Verizon to Pay for Patents," *Wall Street Journal*, June 12, 2019, at https://www.wsj.com/articles/huawei-presses-verizon-to-pay-for-patents-11560354414.

[269] Gwenaelle Barzic, "Europe's 5G to cost $62 billion more if Chinese vendors banned: telcos," *Reuters*, June 7, 2019, at https://www.reuters.com/article/us-huawei-europe-gsma/europes-5g-to-cost-62-billion-more-if-chinese-vendors-banned-industry-idUSKCN1T80Y3.

[270] BT Group plc, 2019 Annual Report, p. 4.

[271] Paul Lipscombe, "Scrapping Huawei could delay UK 5G rollout by up to two years," *Mobile News*, March 25, 2019.

[272] Ray Le Maistre, "BT's McRae: Huawei Is 'the Only True 5G Supplier Right Now,'" *Light Reading*, November 21, 2018, at https://www.lightreading.com/mobile/5g/bts-mcrae-huawei-is-the-only-true-5g-supplier-right-now/d/d-id/747734.

[273] Michelle Toh, "America's fight with Huawei is messing with the world's 5G plans" *CNN Business*, February 15, 2019, at https://edition.cnn.com/2019/02/14/tech/huawei-nokia-ericsson-5g/index.html.

i. Estimating the Effect of 5G Penetration on GDP

164. To estimate the effect of delayed 5G penetration on GDP, I first apply regression analysis to estimate the effect of 4G penetration on GDP. It is likely that the impact on GDP per capita of the transition from 4G to 5G will be at least as great as the impact on GDP per capita of the transition from 3G to 4G. One of the reasons that the transition to 5G would have a greater impact than did the transition to 4G is the substantial network effects that are predicted to be generated by billions of devices connected to 5G networks, as well as the virtuous cycle generated by the other applications of 5G discussed in Section IV.

165. To perform this estimation, I apply data from GSMA Intelligence on 4G penetration rates and total mobile penetration rates in Australia, Canada, Germany, Japan, South Korea, the United States, and the United Kingdom over the years 2012 to 2017. To isolate the effect of 4G wireless penetration on GDP I control for other factors, including the country's overall wireless penetration rate, country's net investment in nonfinancial assets, country's total supply of labor, and volume of trade measured as the sum of imports and exports. These variables, as well as data on GDP per capita, are taken from the World Bank's World Development Indicators ("WDI") database.[274]

166. My regression specification follows the regression specification developed in the 2012 Deloitte study[275] that I described in Section VIII.B, which estimated the effect of 3G penetration on GDP per capita.

167. I find that a one percentage point increase in the 4G penetration rate increased GDP per capita by 0.035 percent all else equal over the countries studied. This result is statistically significant and robust to modifications in the model specification. Details of this estimation are provided in Appendix B.

[274] See "Databank. World Development Indicators," World Bank, at https://databank.worldbank.org/data/source/world-development-indicators.

[275] "What is the impact of mobile telephony on economic growth? A Report for the GSM Association." Deloitte, November 2012, pp. 13-14.

168. To put this result into context, an increase of 1 percent in the 4G penetration rate would have increased total GDP in Q2 2019 by approximately $7.5 billion, according to this estimate.[276]

ii. Modeling the Delay Due to the Absence of Huawei

169. Because it is impossible to predict precisely the extent of delay in 5G penetration that will result from Huawei's absence from the United States, I quantified the effects of delay under three reasonable delay scenarios. The estimates of delay time are based on reports of Huawei's 5G equipment advances over other vendors' 5G equipment and estimates by other observers already discussed in this report of delays due to the exclusion of Huawei from the U.S. market for RAN equipment.[277] These factors have led me to quantify the losses to the U.S. economy from delayed 5G penetration of 6, 12, and 18 months due to Huawei's absence from the U.S. market. My estimates quantify the effects of these delays over and above the effect of the delay already caused by and anticipated due to the U.S. spectrum gap.

170. Delayed entry of a product or service of a firm into a market may or may not have persistent effects as a general economic matter. For example, delayed entry by one product or service of a firm into an established market in which this firm already sells other products or services may have little or no persistent effects on that firm's ability to sell its product or service, depending on characteristics of the market, firm, distribution channels, and product or service. However, in some cases, delayed entry may accelerate the penetration rate of the delayed product or service offered by the later mover if the first mover has educated customers about the product category or technology, thereby overcoming initial resistance

[276] $7,468,237,717.5=$64,830*0.01*0.035*329,135,000. See "Population, Thousands, Quarterly, Not Seasonally Adjusted," Federal Reserve Bank of St. Louis, accessed August 16, 2019, at https://fred.stlouisfed.org/series/B230RC0Q173SBEA; "Gross domestic product per capita, Dollars, Quarterly, Seasonally Adjusted Annual Rate," Federal Reserve Bank of St. Louis, accessed August 19, 2019, at https://fred.stlouisfed.org/series/A939RC0Q052SBEA.

[277] See Section VIII.D.

to it, for example.[278] The existence, absence, or extent of persistent effects of delay are a factual matter that depend on the market circumstances.

171. The history of adoption at a national level of new generations of wireless technology buildout indicates that when infrastructure buildout is delayed and penetration of the technology is depressed, the delay will generally have persistent consequences. This is not surprising, because penetration of a new wireless technology such as 4G or 5G requires network buildout and capital expenditure location by location. Typically, carriers have neither the capital nor managerial capabilities to build out a new generation network at all nationwide locations simultaneously; rather, buildout occurs sequentially, beginning with most attractive or otherwise most feasible locations first. As a result, delaying the initiation of network upgrades sets back the entire trajectory of upgrades and, therefore, adoption of the new technology. Depressing nationwide adoption of a new generation of wireless technology in one quarter, for example, will affect the trajectory of adoption over future quarters, and it may take many years for the penetration rate to catch up to the level it would have achieved had it begun earlier.

172. To assess empirically the persistence of delayed deployment by a country of a new generation of wireless technology infrastructure, I performed an analysis of 4G penetration rate data for 8 countries over the Q1 2006-Q4 2018 period, depicted earlier in Figure VIII.1. Details of this analysis are provided in Appendix B.i. I found that delayed deployment of a new wireless technology does indeed have persistent effects over time and that while the effect varied from country to country, countries that were delayed in deployment of 4G tended not to catch up to earlier deployers for several years.

173. Based on the results of my data analysis, I assume that the impact of an initial delay in infrastructure deployment on overall penetration of the new technology generation will persist for five years and one quarter before the United States attains the penetration level it would have achieved but for the initial delay. That is, an initial delay of, for example,

[278] Theo Anderson, "The Second-Mover Advantage," based on the research of Venkatesh Shankar and Gregory Carpenter, Kellogg Insight, November 4, 2013, at https://insight.kellogg.northwestern.edu/article/the_second_mover_advantage.

six months would result in 5G penetration being six months behind the level it would otherwise have achieved at each point in time for five years and one quarter, after which time the 5G penetration rate reaches the 5G penetration rate the United States would have achieved but for the initial delay.[279]

iii. Calculation of the Effect of Delayed 5G Deployment on the U.S. Economy Due to Exclusion of Huawei

174. My purpose is to estimate the effect of delayed deployment due to Huawei's exclusion from the United States while also taking into account, and controlling for, the fact that the United States is also suffering a delay in 5G deployment due to the U.S. spectrum gap. Specifically, my methodology estimates the effect of the delay due to exclusion of Huawei over and above the effect on the economy of the delay due to the spectrum gap.

175. Hence, to estimate the effect on 5G penetration of a deployment delay in the United States due to Huawei's absence from the U.S. market, I first estimated the loss to the U.S. economy associated with a delay due to the spectrum gap in the United States alone.

176. U.S. carriers started deploying (very limited) 5G mobile commercial networks using spectrum available to them in Q1 2019.[280] Only when the FCC releases mid-band spectrum to carriers can all U.S. carriers start deploying 5G networks on a broad basis. I assume that had mid-band spectrum been available to all major U.S. carriers, they would have started deploying 5G on a broad basis in Q1 2019. The FCC has not yet set a date to release mid-band spectrum to major U.S. carriers, but FCC commissioner Ajit Pai has announced that the FCC intends to do so in 2019 or 2020.[281] I assume that mid-band spectrum will be made available to carriers in Q3 2019. If this schedule holds, the delay associated with the

[279] This analysis is based on GSMA data on 4G penetration rates for Australia, Canada, China, Germany, Japan, South Korea, the United Kingdom, and the United States over Q4 2006-Q4 2018.

[280] See Appendix D.

[281] Specifically, in June 2019 Ajit Pai said in his testimony before the U.S. Senate Committee on Commerce, Science, and Transportation that "we intend to take action to make available more spectrum in the 2.5 GHz and 3.7-4.2 GHz bands in the coming months." He also stated that in 2020 the FCC intends to auction spectrum in the 3.5 GHz band and that the FCC expects to authorize initial commercial deployments in this band in summer 2019. Statement of Chairman Ajit Pai, Federal Communications Commission, Hearing on "Oversight of the Federal Communications Commission," Before the United States Senate Committee on Commerce, Science, and Transportation, June 12, 2019, available at https://docs.fcc.gov/public/attachments/DOC-357959A1.pdf.

spectrum gap will be approximately 6 months;[282] therefore, in my model I assume that the delay in deployment of 5G networks in the United States due to the U.S. spectrum gap is 6 months.[283]

177. Second, I estimate the losses to the U.S. economy associated with the cumulative delay due to the spectrum gap (6 months) and Huawei's continued exclusion (an additional 6, 12, or 18 months).

178. To calculate the incremental loss due to delay associated with Huawei's absence, I subtract the estimated loss due to delay associated with the spectrum gap from the estimated loss due to the cumulative delay associated with both the spectrum gap and Huawei's absence.

179. To perform these calculations, I model the 5G penetration rate in a scenario with no delay at all from Q2 2019 to Q1 2026 that would occur in the United States as following the same growth path as did the U.S. 4G penetration rate from Q1 2009 to Q4 2015.[284] I assume, however, that when deployment is delayed by time t, the penetration rate is also delayed by time t, and that the delay in penetration rate persists for five years and one quarter from the start of deployment, as discussed earlier. Figure VIII.2 shows the modeled trajectories

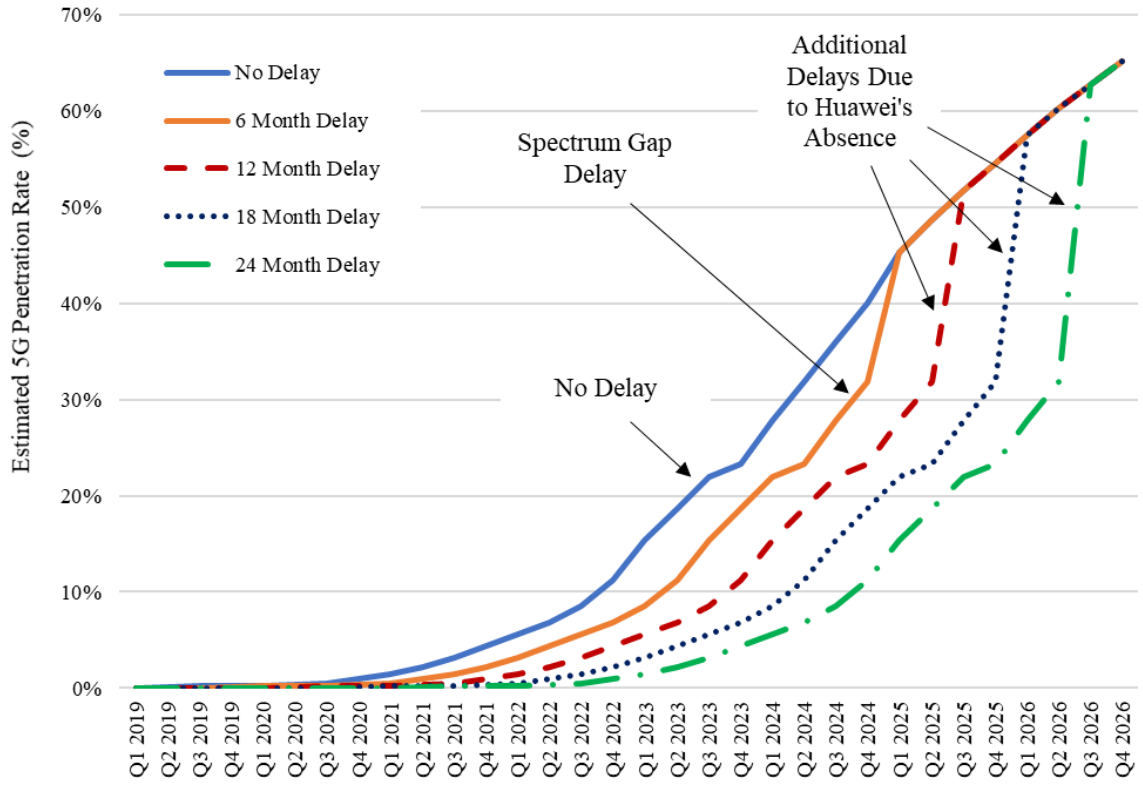
[282] Because the availability of 5G networks is very limited as of the writing of this report, I assume that 5G the penetration rate will remain close to zero until after mid-band spectrum is made available to carriers. See Appendix D for the state of 5G deployment in the U.S.

[283] The duration of delay associated with the spectrum gap is likely to be longer than 6 months, because generally spectrum reallocation is a long and complicated process. Even if the delay due to the spectrum gap is longer than 6 months, however, the additional delay in deployment due to Huawei's absence from the market is unlikely to shrink, because as Huawei and all other vendors continue to invest in continued development, Huawei is likely to preserve its technological lead over the other vendors of RAN equipment. I estimated losses associated with a longer spectrum gap and the same durations of delay due to Huawei's absence and found that the losses increase when the spectrum gap increases. Note that when the spectrum gap increases, the cumulative delay associated with the spectrum gap and Huawei's absence from the U.S. market may affect the penetration rate of 5G beyond 2024. Therefore, comparing the costs due to Huawei's absence from the U.S. market in the scenarios with longer spectrum gap delays requires estimating the decline in GDP over longer periods of time. For example, if the spectrum gap delay increases by 6 months (i.e., the spectrum gap is 12 months in total), assuming the same additional delay durations due to Huawei's absence, the economic losses to the U.S. over 2019-2026 increase by $19-50 billion depending on the duration of the additional delay due to Huawei's absence. My analysis is, therefore, conservative.

[284] Although the first 5G networks in the U.S. have launched, the availability of 5G remains very limited. Because no statistics on 5G subscribership are available in the U.S., I consider this to be a signal that there are very few 5G subscribers in the U.S. For the purposes of my model, I assume that the 5G penetration rate will remain close to zero until after mid-band spectrum is released to U.S. carriers. I assume that in a scenario with no delay (due to the spectrum gap or Huawei's absence from the U.S. market), the adoption of 5G in the U.S. would have started in Q2 2019, because this is when the first U.S. carrier Verizon launched its 5G mobile network using high-band spectrum.

of 5G penetration rate (1) in the scenario without any delay; i.e., a world in which the United States experienced no delay even due to the spectrum gap or due to an absence of Huawei from the market; (2) in the scenario in which the United States experiences the delay associated with the spectrum gap but no additional delay due to the absence of Huawei; and (3) in the scenarios with 12, 18, and 24 months delay, which result from the cumulative delay due to the spectrum gap and Huawei's absence from the U.S. market for RAN equipment.

Figure VIII.2
Estimated 5G Penetration Rate in the U.S. without Delay and with Delays of 6, 12, 18, and 24 Months Due to Spectrum Gap and Due to Absence of Huawei from the U.S. Market



Notes:
[1] I assume that without a delay in 5G deployment, the 5G penetration rate between Q2 2019 and Q4 2026 will replicate the 4G penetration rate between Q1 2009 and Q3 2016. I assume that if 5G deployment were delayed, the 5G penetration rate would follow the same trajectory as in the scenario without delay, but its start would be delayed by the time equal to the duration of delay and will remain delayed for twenty-one quarters, or 5.25 years, from the start of deployment in the scenario with delay; I assume that after 5.25 years, the 5G penetration rate in the scenario with delay will be equal to the 5G penetration rate in the same quarter from the scenario without delay. For example, when 5G deployment is delayed by six months, the 5G penetration rate is assumed to be zero in Q2 2019 and Q3 2019; for t = Q4 2019-Q4 2024 it is assumed that the 5G penetration rate in Q_t equals the 5G penetration rate from the scenario without delay in Q_{t-2}; and for t = Q1 2025-Q4 2026 it is assumed that the 5G penetration rate in Q_t equals the 5G penetration rate from the scenario without delay in Q_t.
[2] The FCC intends to release mid-band spectrum to carriers in 2019-2020, but no date has been set. I assume that mid-band spectrum will be released to carriers in Q3 2019; therefore, I assume that the delay associated with the spectrum gap is 6 months. I discuss the implications of a longer delay due to a spectrum gap in fn. 281.

Sources:
[1] GSMA Intelligence, "Country Dashboard," 2019, for the United States.
[2] Statement of Chairman Ajit Pai, Federal Communications Commission, Hearing on "Oversight of the Federal Communications Commission," Before the United States Senate Committee on Commerce, Science, and Transportation, June 12, 2019, available at https://docs.fcc.gov/public/attachments/DOC-357959A1.pdf.

180. To calculate the percentage point decline in the 5G penetration rate because of delay under each of my defined delay scenarios, I first calculated the average annual 5G penetration rate in the scenario with delay and without delay and then subtract the 5G penetration rate that would occur in the delay scenario from the 5G penetration rate that would occur if there were no delay in each year in which the delay is expected to persist. I limited my analysis to the 2019-2024 period.[285]

181. To calculate the effect of that reduced penetration on GDP, I multiplied my regression estimate of the effect on GDP per capita of a reduction in 5G penetration rate by the calculated decline in 5G penetration rate in each year. The product is the estimated percentage decline in GDP per capita in each year due to delay. I multiplied this percentage decline by the projected GDP per capita in that year to get an estimate of the decline in GDP per capita due to delay.

182. I translated the resulting estimated decline in per capita GDP into the estimated decline in total GDP by multiplying the estimated loss in GDP per capita by the projected population of the United States in each year.

183. The total reduction in GDP for each delay scenario is the sum of the GDP reductions in each year associated with that delay scenario discounted to 2019 at a social discount rate of 3.5 percent, as provided by economists Mark Moore and Aidan Vining for the United States [286]

184. Finally, to isolate the losses resulting from the absence of Huawei, I subtracted the estimated reduction in GDP resulting from the spectrum gap alone from the estimated reduction in GDP resulting from the cumulative delay due to the spectrum gap and

[285] In the scenario with the shortest duration of delay due to Huawei's absence from the U.S. market, I project that the U.S. catches up with the penetration rate in no delay scenario in Q1 2025. To simplify my analysis, I calculate losses for all delay scenarios over the 2019-2024 period.

[286] Social discount rate is the rate that is used in a cost-benefit analysis of a potential regulation or public project to calculate that project's net present value. The social discount rate is the annual percentage decline in a representative individual's utility from consuming the same bundle of goods or services in the future as opposed to the present. Mark A. Moore and Aidan R. Vining, "The Social Rate of Time Preference and the Social Discount Rate," *Mercatus Center: George Mason University* (2018), pp. 3 and 5, at https://www.mercatus.org/system/files/moore_and_vining_-_mercatus_research_-_a_social_rate_of_time_preference_approach_to_social_discount_rate_-_v1.pdf.

Huawei's exclusion. For example, to calculate the reduction in GDP caused by a 6-month delay due to a Huawei's absence, I estimate the cost resulting from a 12-month delay (a 6-month delay due to the spectrum gap plus a 6-month delay due to Huawei's exclusion) and subtract from it the estimated reduction in GDP associated with the 6-month delay resulting from spectrum gap alone. The detailed calculations are shown in Appendix B and Exhibit B.2.

185. The results of this analysis are presented in Exhibit VIII.1.

186. Exhibit VIII.1 shows that the impact of a delay in 5G deployment is substantial. Depending on the extent of the delay, the present discounted value of losses to the U.S. economy from Huawei's absence varies from approximately $104 billion (from a 6-month delay) to approximately $241 billion (from an 18-month delay) over the duration of delay. These estimated losses are over and above the costs to the economy associated with the spectrum gap alone.

Exhibit VIII.1
Total Losses Resulting from the Delay of 5G Deployment to the United States under Different Delay Scenarios, Discounted Present Value

Delay Duration	Decline in Total GDP Due to Delay Caused by Absence of Huawei, 2019-2024
6 Months	$ 103,646,561,838
12 Months	$ 182,024,710,760
18 Months	$ 240,671,885,050

Note: See notes and sources to Exhibit B.2.

iv. Calculation of the Effect of Delayed 5G Deployment on U.S. Employment Due to Exclusion of Huawei

187. Delayed deployment of 5G will have a ripple effect on the U.S. economy that will affect not only GDP but employment as well. Investment in the deployment of 5G networks will create new jobs that are required to deploy 5G networks and to support the additional goods and services whose purchase will be stimulated by those workers' income throughout the United States. Correspondingly, delayed 5G deployment means that some jobs will not be

created in the years in which investment spending on deployment is depressed. In this section I estimate the effect of investment in 5G RAN deployment on U.S. employment in years in which investment spending is depressed in the three delay scenarios—2019, 2020, and 2021.

188. Delay in 5G deployment will directly affect employment in industries related to the roll-out of 5G networks, such as construction, engineering, and others directly involved in the deployment of networks. Jobs lost in these industries are "direct" jobs lost.[287] Reduced employment in one industry also affects the employment in other industries. When jobs are lost in one industry and the output of that industry falls, other industries that supply inputs to that industry also lose jobs. These are "indirect" jobs lost.[288] In addition, jobs supported by the demand for goods and services purchased using the incomes of workers in these direct and indirect jobs will also suffer. For example, jobs in the construction industry support jobs at restaurants and grocery stores where employees engaged in construction and related activities eat and shop for food. These are "induced" jobs lost.[289] The sum of the effects on direct, indirect, and induced jobs is the total effect on employment of investment in 5G deployment.

189. The total effect of investment spending in a specific industry on employment is commonly estimated using so-called "input-output" multipliers, which show how many direct and indirect jobs are generated per $1 million in investment spending in a given industry. The input-output multipliers I apply in my analysis do not include induced effects on employment, which makes my estimate conservative.[290] To calculate how many jobs will be lost in 2019-2021 because of the delay in investment in 5G infrastructure, I use

[287] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," Analysis Group, February 2019, p. 12.

[288] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," Analysis Group, February 2019, p. 12.

[289] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," Analysis Group, February 2019, p. 12.

[290] As I explain in this section, I use employment multipliers provided by the Bureau of Labor Statistics, and they do not include induced multiplier effects. See Richard W. Graham, "Employment Outlook: 2018-2028. Layout and Description For 205-Order Employment Requirements Tables: Historical 1997 through 2018," prepared in the Bureau of Labor Statistics Office of Occupational Statistics and Employment Projections, September 4, 2019, p. 6, at https://www.bls.gov/emp/data/emp-requirements.htm.

multipliers from what are called employment requirements tables, which are developed by the U.S. Bureau of Labor Statistics ("BLS"), an agency of the U.S. Department of Labor. These tables are provided annually, and they are based on the input-output tables developed by the U.S. Bureau of Economic Analysis ("BEA") supplemented with data from additional sources, such as data from the U.S. Census Bureau and from the U.S. Department of Agriculture.[291] These tables allow one to estimate the effect of spending on one industry's final goods and services on overall U.S. employment.[292,293] I use these multipliers to estimate how many more jobs would have been generated between 2019 and 2021 but for the delay in 5G investment due to the absence of Huawei from the U.S. market for RAN equipment.

190. Investment in 5G RAN infrastructure is not just an investment in one particular industry; instead, it involves investment in several industries. I rely on existing economic studies to

[291] Richard W. Graham, "Employment Outlook: 2018-2028. Layout and Description For 205-Order Employment Requirements Tables: Historical 1997 through 2018," prepared in the Bureau of Labor Statistics Office of Occupational Statistics and Employment Projections, September 4, 2019, at https://www.bls.gov/emp/data/emp-requirements.htm.

[292] Economists also use RIMS II multipliers developed by the BEA to estimate the potential effects of various projects, such as investment in new infrastructure (e.g., building a new road or stadium) on regional economies' employment and output. The BEA, however, does not provide nationwide RIMS II multipliers. RIMS II multipliers are only available for states and counties. For this reason, I use multipliers provided by the BLS. See "RIMS II: An essential tool for regional developers and planners," Bureau of Economic Analysis, U.S. Department of Commerce, pp. iii, 1-1, at https://www.bea.gov/resources/methodologies/RIMSII-user-guide; "Frequently Asked Questions," Bureau of Economic Analysis, U.S. Department of Commerce, at http://commercedataservice.github.io/BEA_RIMS_Redesign/faq-page.html.

[293] The BLS notes that there are several limitation to the multipliers that it provides: (1) BLS assumes that the input-output relations are stable over time, which may not hold, especially in the long-run; (2) the price deflator applied by the BLS to the tables to remove the effects of relative price changes over time may cause distortions of data in the tables; (3) the estimated effect on employment using the BLS multiplier may include both part- and full-time jobs; (4) the effect estimates an increase in jobs and not an increase in employment; (5) the employment factors may vary even though the true productivity may or may not have changed; (6) the input-output tables do not distinguish between domestically produced and imported goods and assume domestic production techniques; these tables may overstate the impact of incremental investment on domestic employment; (6) the estimated relationships using input-output matrices are average relationships which may not hold on the margin; and (7) the input-output multipliers do not include the impact of spending on consumer goods and services that is funded by these workers' incomes generated by producing the goods and services. See Richard W. Graham, "Employment Outlook: 2018-2028. Layout and Description For 205-Order Employment Requirements Tables: Historical 1997 through 2018," prepared in the Bureau of Labor Statistics Office of Occupational Statistics and Employment Projections, September 4, 2019, at https://www.bls.gov/emp/data/emp-requirements.htm, pp. 5-6.

identify the industries involved in 5G RAN infrastructure deployment.[294] Specifically, I rely on a study by economists Jeffrey Eisenach, Hal Singer, and Jeffrey West which identifies the following industries involved in broadband deployment: (1) telephone apparatus manufacturing, (2) broadcast and wireless communications equipment, (3) fiber optic cable manufacturing, and (4) construction.[295] To estimate the share of investment spending on the goods and services of each industry, I rely on the methodology proposed by the Analysis Group study and calculate industry spending shares as the average of investment spending shares for broadband deployment estimated for the fiber-to-the-home industry and the wireless industry from the study by economists Jeffrey Eisenach, Hal Singer, and Jeffrey West.[296] See Exhibit VIII.2.

[294] I assume that the deployment of 5G RAN will require investment in the same industries in the same proportions as total 5G deployment.

[295] Jeffrey A. Eisenach, Hal J. Singer, & Jeffrey D. West, "Economic Effects of Tax Incentives for Broadband Infrastructure Deployment," Empiris LLC, prepared on behalf of the Fiber-To-The-Home Council (2009), p. 8.

[296] Jeffrey A. Eisenach, Hal J. Singer, & Jeffrey D. West, "Economic Effects of Tax Incentives for Broadband Infrastructure Deployment," Empiris LLC, prepared on behalf of the Fiber-To-The-Home Council (2009), p. 8; David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," Analysis Group, February 2019, pp. 11-12 and Figure A-3.

Exhibit VIII.2
Shares of Investment Spending on 5G Infrastructure by Industry

Industry NAICS Code	Industry Name	Investment Spending Shares		Investment Spending Shares for 5G Infrustucture Investment
		Fiber-to-the-Home ("FTTH") Industry	Wireless Industry	
[A]	[B]	[C]	[D]	[E]=([C]+[D])/2
334210	Telephone apparatus manufacturing	30%	0%	15%
334220	Broadcast and wireless communications equipment	0%	93%	46.5%
335921	Fiber optic cable manufacturing	20%	0%	10%
230000	Construction	50%	7%	28.5%

Notes:
[1] I follow the same methodology as Sosa and Rafert (2019) in calculating weights of 5G infrastructure spending for the four industries as the average of the investment spending shares to the Fiber-to-the-Home and Wireless industries from Eisenach, Singer, and West (2009) paper.
[2] NAICS codes are North American Industry Classification System codes which are adopted by the U.S. Bureau of Economic Analysis and U.S. Bureau of Labor Statistics in their input-output data.

Sources:
[1] Jeffrey A. Eisenach, Hal J. Singer, and Jeffrey D. West, "Economic Effects of Tax Incentives for Broadband Infrastructure Deployment," Empiris LLC, prepared for Fiber-to-the-Home Council (2009), p. 8.
[2] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, Table A-3, p. 11.

191. Next, I use employment multipliers provided by the BLS for each of these industries and investment shares estimated in Exhibit VIII.3 to calculate a weighted average multiplier that I can apply to overall 5G RAN investment spending to estimate the incremental effect of 5G RAN investment spending on U.S. employment.

192. Three out of the four industries identified by Jeffrey Eisenach, Hal Singer, and Jeffrey West and included in Exhibit VIII.2 use six-digit North American Industry Classification System ("NAICS") codes. The BLS does not provide multipliers for detailed industries with six-digit level NAICS codes "334210," "334220," and "335921." The BLS provides data for more aggregated industries with four-digit level NAICS codes "3342" and "3359" which

contain within them the three detailed industries specified above.[297] I then used employment multipliers provided by the BLS for these two industries and for the construction industry (NAICS code "23") and applied spending shares from Exhibit VIII.2 to calculate the weighted average multiplier of 5G RAN investment on employment. I estimate that each $1 million in spending on 5G RAN deployment creates 4.73 jobs. See Exhibit VIII.3.[298]

[297] Richard W. Graham, "Employment Outlook: 2018-2028. Layout and Description For 205-Order Employment Requirements Tables: Historical 1997 through 2018," prepared in the Bureau of Labor Statistics Office of Occupational Statistics and Employment Projections, September 4, 2019, at https://www.bls.gov/emp/data/emp-requirements.htm, p. 1 and the "SectorPlan312.xlsx" data file provided by the BLS; "North American Industry Classification System," United States, 2017, Executive Office of the President, Office of Management and Budget, pp. 31-32, 43, 44-45.

[298] The Analysis Group study estimated the employment multiplier for 5G deployment spending to be 8.66. This multiplier, according to the authors of this study, includes direct, indirect, and induced effects, whereas my estimated multiplier of 4.73 includes only direct and indirect effects and is therefore smaller compared to the Analysis Group estimate. See David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," Analysis Group, February 2019, pp. 11-12, Table A-3.

Exhibit VIII.3
Calculation of a Weighted Average Multiplier of 5G Infrastructure Investment on Employment

Industry NAICS Code	Industry Name	Investment Spending Share	Input-Output Employment Multiplier
3342	Communications equipment manufacturing	61.5%	2.93
3359	Other electrical equipment and component manufacturing	10.0%	6.07
23	Construction	28.5%	8.15
Weighted Average Multiplier			**4.73**

Notes:
[1] The data provided by the Bureau of Labor Statistics are only available for aggregated four-digit NAICS industry codes. I used aggregated industry input-output employment multipliers to calculate the weighted average input-output multiplier.
[2] The investment spending share for industry 3342 was calculated as the sum of investment spending shares for industries 334210 and 334220 from Exhibit VIII.2.

Sources:
[1] Exhibit VIII.2.
[2] Employment Requirement Matrix file "NOMINAL_EMPREQ_2018.csv," Bureau of Labor Statistics, U.S. Department of Labor, available at https://www.bls.gov/emp/data/emp-requirements.htm.
[3] Industry sectoring plan descriptions from "SectorPlan312.xlsx," Bureau of Labor Statistics, U.S. Department of Labor, available at https://www.bls.gov/emp/data/emp-requirements.htm.
[4] "North American Industry Classification System," United States, 2017, Executive Office of the President, Office of Management and Budget, pp. 31, 43, 44.

193. The Analysis Group study estimated that the total investment required to deploy 5G networks in the U.S. over a seven-year period would be $297.92 billion.[299] A report by Frontier Economics assumes that investment spending on RAN networks accounts for 25 percent of the total 5G investment.[300] Applying this estimate to the total 5G investment yields $74.48 billion investment in 5G RAN. Applying the weighted average multiplier

[299] The investment required for 5G deployment is estimated for five large U.S. providers: Verizon, AT&T, Sprint, T-Mobile, and U.S. Cellular. The amount of investment in 5G deployment is estimated based on the inflation-adjusted average capital spending of these five carriers from 2008 to 2017. See David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, pp. 7-9 and Figure A-1.
[300] "The value of competition to 5G network deployment," Frontier Economics, August 2018, p. 41.

from Exhibit VIII.3 to the estimate of 5G RAN investment yields 352.4 thousand job-years over the seven-year period, or 50.3 thousand jobs annually.[301]

194. If Huawei is absent from the U.S. market, a delay in 5G investment of 6 months would result in the loss of 25.2 thousand jobs in 2019. A delay in 5G investment of 12 months would result in the loss of 25.2 thousand jobs in 2019 and 25.2 thousand jobs in 2020. A delay of 18 months would result in the loss of 25.2 thousand jobs in 2019 and 50.3 thousand jobs in 2020. These results are summarized in Exhibit VIII.4.

[301] The total number of generated jobs over the seven-year period of deployment is calculated as follows: 352,442=$297,920,000,000*0.25*4.732 /$1,000,000. The number of generated jobs per year is calculated as follows: 50,349=352,442/7.

Exhibit VIII.4
Decline in Employment Due to Huawei's Absence from the U.S. Market for RAN Equipment under Different Delay Duration Scenarios

Delay Duration Due to Huawei's Absence	Decline in Employment Due to Absence of Huawei (in Number of Jobs)		Total Jobs Lost
	2019	2020	
6 Months	25,174	-	25,174
12 Months	25,174	25,174	50,349
18 Months	25,174	50,349	75,523

Notes:
[1] Under the 6-month delay scenario, deployment is delayed from Q3 2019 to Q1 2020; under the 12-month delay scenario, the deployment is delayed from Q3 2019 to Q3 2020; under the 18-month delay scenario, the deployment is delayed from Q3 2019 to Q1 2021. I calculate the employment effect only over the period in which 5G networks would have begun deployment in the presence of Huawei but would not in its absence; I conservatively assume that no jobs will be lost due to lower investment in 5G networks in any other quarter.
[2] Jobs lost in year *i* in each delay scenario are calculated as follows: 50,349 (number of jobs lost per year)*delay duration in months in year *i*/12 months, where *i* equals 2019 or 2020. For example, in the case of a 6-month delay, the delay in deployment starts in Q3 2019 and ends in Q1 2020; therefore, the number of jobs lost in 2019 equals 50,349*6/12 = 25,174. No jobs are lost in 2020 because there is no delay in deployment in this year under the scenario of 6-month delay.

Sources:
[1] David W. Sosa and Greg Rafert, "The Economic Impacts of Reallocating Mid-Band Spectrum to 5G in the United States," *Analysis Group*, February 2019, pp. 7-9, 11-12.
[2] Exhibit VIII.3.
[3] "The value of competition to 5G network deployment," Frontier Economics, August 2018, p. 41.

IX. THE IMPACT ON THE COSTS OF RAN EQUIPMENT DUE TO REDUCED COMPETITION FROM EXCLUDING HUAWEI FROM THE U.S. MARKET FOR RAN NETWORK EQUIPMENT

195. In addition to the effects of excluding Huawei from the United States on GDP and employment due to the expected delay in investment in and adoption of 5G technology, continued exclusion of Huawei would harm the U.S. economy by reducing competition in the sale of 5G equipment relative to what it would be if Huawei were active in the U.S. market.

196. The current exclusion of Huawei has already increased market concentration in the U.S. market for RAN equipment and has likely substantially increased prices of RAN equipment in the U.S., as I show below. Going forward, the impact on market concentration and prices of RAN equipment, including 5G RAN equipment, may be somewhat greater, because additional restrictions imposed on Huawei's presence in the U.S. are likely to erode Huawei's already negligible revenue share in the U.S. market for RAN equipment.

197. As a general economic matter, it is to be expected that the marketplace for 5G RAN equipment, and for RAN equipment in general, would be more competitive if Huawei were in the market than if it continues to be absent from the market. As documented earlier, U.S. sales of wireless RAN equipment are highly concentrated among only two major vendors.[302] In the rest of the world, the market is generally served by three or more providers who have material revenue shares, and a significant share of the revenue accounted for by Huawei.[303] Huawei's substantial contribution to the market demonstrates that carriers have concluded that, in many circumstances, Huawei offers the best combination of price, service, and quality.

198. The participation of a respected vendor in the marketplace generally has the effect of invigorating competition among all of the participants. As a result, even if a purchaser selected a competitor other than Huawei, the additional competition from Huawei can drive the price offered by the other competitors down relative to the price they would have charged in the absence of the additional competition from Huawei.[304] For example, economist Allan Shampine found that higher industry concentration in North America is associated with higher prices for RAN equipment in general and for LTE base stations in particular, though he did not provide a quantification of the effect.[305]

---

[302] See Section VI.

[303] Based on data provided by Dell'Oro Group.

[304] The additional competition can have additional beneficial effects on the marketplace, including accelerating innovation that is targeted to the needs of U.S. carriers. I discussed this effect in previous sections and do not estimate these effects in this section.

[305] Comments of Allan L. Shampine, Ph.D. On "Competition and Consumer Protection in the 21st Century Hearings, Project Number P181201," August 20, 2018, p. 10.

199. The question of how to quantify the effect of reducing competition in a market arises commonly in the context of analyzing potential mergers. A merger is similar to an exclusion of a competitor in the sense that the number of independent competitors serving a market is lower if the merger is permitted than if the merger is precluded. To determine whether a merger is likely to have adverse effects on a market, economists have developed well-accepted methodologies for estimating the effect on prices of the elimination of a competitor.[306]

200. To evaluate the effects of eliminating a competitor from the market in a case of merger, economists and regulatory agencies often analyze market concentration.[307] The Herfindahl-Hirschman Index ("HHI") is an accepted measure of concentration.[308] The HHI is calculated by summing the squares of the individual firms' market shares.[309] The HHI ranges from close to zero for a market with a large number of small competitors, to 10,000 for a pure monopoly.

201. When market concentration significantly increases as a result of a merger (or exclusion of a competitor) and results in a highly concentrated market, such a merger raises concerns that the increased concentration will cause prices to increase significantly by increasing the market power of the remaining firms.[310]

202. The 2010 Horizontal Merger Guidelines classify markets into three types based on the value of the market's HHI:

- HHI below 1,500 – unconcentrated markets;

---

[306] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3, 6-6.1; Carl Shapiro, "Mergers with Differentiated Products," *Antitrust*, Spring 1996, pp. 24-28, at http://faculty.haas.berkeley.edu/shapiro/diversion.pdf.

[307] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3. Market concertation evidence is considered in conjunction with other evidence of competitive effects, including ease and timeliness of potential entry into the market.

[308] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3.

[309] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3.

[310] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 2.1.3.

- HHI between 1,500 and 2,500 – moderately concentrated markets; and
- HHI above 2,500 – highly concentrated markets.[311]

203. According to the 2010 Horizontal Merger Guidelines, mergers resulting in highly concentrated markets and that increase the HHI by 100 to 200 points "potentially raise significant competitive concerns and often warrant scrutiny."[312] Mergers that result in highly concentrated markets and that increase the HHI by more than 200 points will be "presumed to be likely to enhance market power," unless proven otherwise.[313]

204. I calculated the HHIs in the market for all RAN equipment in each region. Exhibit IX.1 shows that the market for all RAN equipment is highly concentrated in each region, but more so in North America than in any other region. The high levels of concentration in North America reflected in Exhibit IX.1 are largely due to the limited presence of Huawei in the United States (discussed in Section VI).

[311] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3.

[312] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3.

[313] "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 5.3.

Exhibit IX.1
RAN Market Concentration by Region, 2018

Region	HHI	Number of Companies
North America	4,045	7
Europe	2,869	6
Middle East & Africa	3,187	5
Asia Pacific	2,568	9
Caribbean & Latin America	3,399	6

Notes:
[1] 5G RAN revenues are not available prior to Q4 2018.
[2] Dell'Oro Group discontinued data collection for CDMA RAN equipment in Q1 2019; data on CDMA RAN include only macro sites in Q2 2018-Q4 2018.
[3] GSM RAN sales include only sales of macro sites and base station controllers ("BSCs") in Q1 2019.

Sources:
[1] "TOTAL GSM," "TOTAL CDMA," "TOTAL WCDMA," "TOTAL LTE," "TOTAL 5G NR," Dell'Oro Group, Q1 2019.
[2] "Mobile RAN Quarterly Report: 1Q19," Dell'Oro Group, Tables 1, 2, and 3.

205. Estimating the effect of increased concentration (i.e., the increase in the HHI) in the United States because of Huawei's limited presence on prices for RAN equipment requires an estimate of vendors' RAN revenue shares assuming Huawei's participation is restricted in the market and an estimate of what vendors' RAN revenue shares would be if Huawei's presence were not restricted by government policies in the U.S. market.

206. Because Huawei has never been allowed to fully participate in the U.S. telecommunications equipment market, as I explained in Section VI, the observed revenue shares of Huawei and other vendors in North America are those in which Huawei is largely absent from the market. I use vendors' revenue shares in sales of all RAN equipment in North America in 2018 to approximate what their revenue shares would be assuming Huawei is restricted from the U.S. market.[314]

207. The revenue shares of Huawei and other vendors in the so-called "but for" world in which Huawei were allowed to fully participate in the U.S. market are not observed. I consider

[314] As I explained in Section VI, vendors' revenue shares in North America primarily reflect vendors' revenue shares in the U.S. This approach assumes that vendors' revenue shares across all generations of wireless RAN are a good approximation for their revenue shares for 5G RAN, both if Huawei were present or absent from the market.

three scenarios for what Huawei's revenue share would be if it were allowed to participate in the U.S. market: (1) Huawei's revenue share would equal its revenue share in Europe, (2) Huawei's revenue share would equal its average revenue share in all regions except North America, and (3) Huawei's revenue share would equal its average revenue share worldwide including the United States.[315]

208. I estimate other vendors' revenue shares in the presence of Huawei using so-called diversion ratios from these vendors to Huawei, which reflect the share of sales that would have been diverted from each vendor to Huawei were Huawei not excluded by policy in the United States[316] The assumed diversion ratio from vendor A to vendor B equals $s_B/(1-s_A)$, where s_A and s_B are revenue shares of vendors A and B, respectively.[317] The details of my analysis are provided in Appendix C.

209. Applying my estimates of revenue shares in the U.S. RAN market with and without Huawei, I estimate that the absence of Huawei from the U.S. market for RAN equipment increases the HHI from 2,964-3,125 to 4,071; i.e., the HHI increases by 945-1,106 points when Huawei is excluded. According to the 2010 Horizontal Merger Guidelines criteria

[315] These data are provided by Dell'Oro Group. Due to the confidentiality of these data, I am not able to provide Huawei's revenue shares in this report.

[316] Estimating diversion ratios from market shares is an approximation that may not be valid if subsets of products in the purported market form submarkets or otherwise are closer substitutes to one another than reflected by the market shares. In such circumstances it would be appropriate to conduct analyses of the cross-price elasticities between the products, data permitting, to obtain more accurate estimates of diversion ratios. In the instant case, however, there is no reason to believe that Huawei's products form a submarket with a subset of the products of the other vendors in the market. My methodology of considering three alternative sets of diversion ratios reflecting three different sets of market shares provides robustness to my estimated price effects. See Carl Shapiro, "Mergers with Differentiated Products," *Antitrust*, Spring 1996, p. 25, at http://faculty.haas.berkeley.edu/shapiro/diversion.pdf.

[317] Carl Shapiro, "Mergers with Differentiated Products," *Antitrust*, Spring 1996, p. 25, at http://faculty.haas.berkeley.edu/shapiro/diversion.pdf.

quoted above, such an increase in HHI would be presumed to enhance market power, cause prices to rise, and damage social welfare.[318]

Exhibit IX.2
Estimated Increase in Concentration in the U.S. Market for RAN Equipment if Huawei's Participation is Restricted in the U.S.

Concentration Estimate	Estimated Increase in Market Concentration if Huawei's Participation Is Restricted in the U.S. Market		
	Scenario 1	Scenario 2	Scenario 3
HHI without Huawei	4,071	4,071	4,071
HHI with Huawei	3,009	3,125	2,964
Increase in the HHI	1,061	945	1,106

Notes:
[1] Scenario 1 assumes that Huawei's revenue share in the U.S. market for RAN equipment if Huawei were allowed in the U.S. market would equal Huawei's revenue share in RAN equipment sales in Europe in 2018. Scenario 2 assumes that Huawei's revenue share in the U.S. market for RAN equipment if Huawei were allowed in the U.S. market would equal Huawei's revenue share in RAN equipment sales in all regions except North America in 2018. Scenario 3 assumes that Huawei's revenue share in the U.S. market for RAN equipment if Huawei were allowed in the U.S. market would equal Huawei's revenue share in RAN equipment sales worldwide in 2018.
[2] The Herfindahl-Hirschman Index ("HHI") in the presence of Huawei in the U.S. market for RAN equipment is calculated as follows: $HHI_H = (rs_{Huawei})^2 + (rs_{Ericsson})^2 + (rs_{Nokia})^2 + (rs_{Samsung})^2 + (rs_{ZTE})^2 + (rs_{Other})^2$, where rs_i denotes the revenue share of vendor *i* in the presence of Huawei in the U.S. market; and the HHI in the absence of Huawei from the U.S. market for RAN equipment is calculated as follows: $HHI_{WH} = (RS_{Ericsson})^2 + (RS_{Nokia})^2 + (RS_{Samsung})^2 + (RS_{ZTE})^2 + (RS_{Other})^2$, where RS_i denotes the revenue share of vendor *i* in the absence of Huawei from the U.S. market. For the purposes of this analysis, I aggregate all vendors except Huawei, Ericsson, Nokia, Samsung, and ZTE into "Other" category and use their aggregate revenue share to calculate the HHI.

Source: Exhibit C.1.

210. The effect on equipment prices of including Huawei in the market would not be isolated to the prices that Huawei itself would contribute to the market, but rather would affect all vendors' prices. In the absence of Huawei, the remaining firms face less pressure to reduce their prices in order to win business than they would face if competing not only with each

[318] Economist John Kwoka tested whether the criteria published in the 2010 Horizontal Merger Guidelines are in fact able to identify mergers that are anticompetitive. Using a sample of 42 merger retrospectives—detailed studies of the actual effects of past mergers on merger outcomes (mostly on prices)—he examined whether mergers that resulted in a highly concentrated market (HHI above 2,500), and where HHI increased by more than 200 points, resulted in price increases. He found that out of the 21 mergers in his sample that satisfy the 2,500/200 criteria, 18 (85.7 percent) resulted in price increases, and only three resulted in price decreases, leading to the conclusion that the 2010 Horizontal Merger Guidelines provide useful criteria for identifying anticompetitive effects. John Kwoka, "The Structural Presumption and the Safe Harbor in Merger Review: False Positives or Unwarranted Concerns?" *Antitrust Law Journal* 81, no. 3 (2017), p. 856-859.

other but also with Huawei.[319] Some of the sales that a vendor would otherwise lose to Huawei by increasing its price would instead remain with the vendor.[320] If the value of sales that would have been lost to Huawei had Huawei operated in the market is substantial, Huawei's absence from the market can result in substantial upward pricing pressure. Conversely, Huawei's presence in a market can generate substantial downward pricing pressure on all of the other competitors.

211. Economists have developed accepted methodologies for estimating the effect on prices that would result from this increased upward pricing pressure.[321] I have applied a methodology developed by an economist Carl Shapiro to estimate the effect on prices in the United States of excluding Huawei from U.S. sales of RAN equipment. This methodology allowed me to estimate the price increase using the data available to me. The results of my analysis of the effect on RAN equipment prices in the United States of excluding Huawei from the U.S. market are shown in Exhibit IX.3.

---

[319] The regulatory agencies consider two types of competitive effects in merger reviews: (1) "coordinated effects" that arise if the merger makes it easier for the merged firm and its rivals to collude and (2) "unilateral effects" that arise if the merger would give the merged firm a unilateral incentive to raise prices and therefore harm consumers. Joseph Farrell and Carl Shapiro, "Antitrust Evaluation of Horizontal Mergers: An Economic Alternative to Market Definition," *The B.E. Journal of Theoretical Economics Policies and Perspectives* 10, iss. 1 (2010), p. 3. I estimate only unilateral effects of excluding Huawei from the market for RAN equipment. To the extent that there were coordinated effects because Huawei was banned from the U.S. market, my analysis would be conservative by not including them.

[310] The regulatory agencies consider two types of competitive effects in merger reviews: (1) "coordinated effects" that arise if the merger makes it easier for the merged firm and its rivals to collude and (2) "unilateral effects" that arise if the merger would give the merged firm a unilateral incentive to raise prices and therefore harm consumers. Joseph Farrell and Carl Shapiro, "Antitrust Evaluation of Horizontal Mergers: An Economic Alternative to Market Definition," *The B.E. Journal of Theoretical Economics Policies and Perspectives* 10, iss. 1 (2010), p. 3. I estimate only the unilateral effects of excluding Huawei from the market for RAN equipment in my analysis. To the extent that there were coordinated effects because Huawei was banned from the U.S. market, my analysis would be conservative by not including them.

[321] See the discussion of several available methodologies for the estimation of the price increases resulting from a merger in Carl Shapiro, "Mergers with Differentiated Products," *Antitrust*, Spring 1996, pp. 24-28, at http://faculty.haas.berkeley.edu/shapiro/diversion.pdf; "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 6.1.

Exhibit IX.3
Estimated Price Increases of RAN Equipment Resulting from Restricting Huawei's Participation the U.S. Market

Vendors	Estimated Increase in Price if Huawei's Participation Is Restricted in the U.S. Market		
	Scenario 1	Scenario 2	Scenario 3
[A]	[B]	[C]	[D]
ERICSSON	16.4%	18.4%	14.6%
NOKIA	14.0%	15.8%	12.5%
SAMSUNG	6.3%	7.3%	5.5%
ZTE	5.6%	6.4%	4.8%
OTHER	5.7%	6.5%	4.9%
Weighted Average Price Increase (%)	**14.2%**	**16.0%**	**12.6%**

Notes:
[1] Scenario 1 assumes that Huawei's revenue share in the U.S. market for RAN equipment if Huawei were allowed in the U.S. market would equal Huawei's revenue share in RAN equipment sales in Europe in 2018. Scenario 2 assumes that Huawei's revenue share in the U.S. market for RAN equipment if Huawei were allowed in the U.S. market would equal Huawei's revenue share in RAN equipment sales in all regions except North America in 2018. Scenario 3 assumes that Huawei's revenue share in the U.S. market for RAN equipment if Huawei were allowed in the U.S. market would equal Huawei's revenue share in RAN equipment sales worldwide in 2018.
[2] The weighted average price increase is calculated as follows:
$pi_{Ericsson}*rs_{Ericsson}+pi_{Nokia}*rs_{Nokia}+pi_{Samsung}*rs_{Samsung}+pi_{ZTE}*rs_{ZTE}+pi_{Other}*rs_{Other}$, where pi_i is the estimated price increase of vendor *i* and rs_i is the revenue share of vendor *i* in the absence of Huawei in the market; *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other. For the purposes of this analysis, I aggregate all vendors except Huawei, Ericsson, Nokia, Samsung, and ZTE into "Other" category.

Source: Exhibit C.1.

212. As the exhibit shows, I estimate that in the absence of Huawei from the market, the prices of smaller vendors (Samsung, ZTE, and other vendors[322]) are 4.8-7.3 percent higher than they would be in Huawei's presence; Nokia's prices are higher by 12.5-15.8 percent; and Ericsson's prices are higher by 14.6-18.4 percent.

213. I estimate that, overall, the increased market concentration resulting from the absence of Huawei from the U.S. market for RAN equipment has resulted in and will continue to result in 12.6-16.0 percent higher weighted average prices for RAN equipment than would be observed in the market if Huawei were competing in the United States.

[322] "Other vendors" means vendors other than Huawei, Ericsson, Nokia, Samsung, and ZTE.

214. An increase of prices of 12.6-16.0 percent is considered material and harmful to social welfare.[323] First, because these price increases constitute a cost increase experienced by wireless carriers, they would discourage and delay deployment of 5G networks.

215. In addition, higher prices for RAN equipment would discourage the upgrade of networks at all for marginal locations where the profitability of network upgrades would be close to zero even at more competitive prices. These locations would include areas where network costs may be higher and/or demand per square mile lower. According to the FCC, such areas often include rural areas, where customers are often underserved by newer technologies. The FCC attributes, at least partially, the lack of advanced broadband networks available to Americans living in rural areas and on Tribal lands to the cost of infrastructure build out:

> The existence of these unserved areas may be attributable, at least partially, to the cost of building infrastructure over long distances in areas with low population density, as well as the lower incomes and higher rates of poverty and unemployment in rural versus urban areas. This translates into fewer revenue generating opportunities for service providers and ultimately affects their incentive to build broadband networks. [footnote omitted][324]

216. As a result, higher costs for 5G equipment may disproportionately harm areas where, by U.S. policy, there is a particular public interest in encouraging deployment of new wireless technology.

217. In addition, cost increases experienced by wireless carriers would be expected to affect the prices that consumers, businesses, and governments pay for wireless services. While it is

[323] For example, the 2010 Horizontal Merger Guidelines consider 5 percent a commonly used benchmark to assess a price increase that is commensurate with a significant lessening in competition. See "Horizontal Merger Guidelines," U.S. Department of Justice and the Federal Trade Commission, August 19, 2010, Sec. 4.1.1-4.1.2. Kwoka concludes that a price increase of 5.8 percent (and perhaps less) is harmful to social welfare. John Kwoka, "The Structural Presumption and the Safe Harbor in Merger Review: False Positives or Unwarranted Concerns?" *Antitrust Law Journal* 81, no. 3 (2017), p. 856.

[324] 2015 Broadband Progress Report and Notice of Inquiry on Immediate Action to Accelerate Deployment, *In the Matter of Inquiry Concerning the Deployment of Advanced Telecommunications Capability to All Americans in a Reasonable and Timely Fashion, and Possible Steps to Accelerate Such Deployment Pursuant to Section 706 of the Telecommunications Act of 1996, as Amended by the Broadband Data Improvement Act*, Before the Federal Communications Commission, GN Docket No. 14-126, FCC 15-10 (Released: February 4, 2015), ¶¶ 133, 143.

beyond the scope of this report to estimate the degree to which wireless carriers would pass through their cost increases to consumers, economic theory tells us that it is reasonable to expect at least some of the cost increase to be passed through in the form of higher end-user prices.

218. Finally, the lessening of competition can also affect the quality of products offered in the U.S. market and the amount of innovation that U.S. consumers enjoy. The competitive effect of higher market concentration due to Huawei's absence from the U.S. RAN market is, therefore, unlikely to be limited only to higher prices of products offered in the United States. For example, without direct competition from Huawei in the United States, Ericsson and Nokia would rationally find it somewhat less pressing to intensify their R&D expenditures and accelerate their R&D efforts to develop better, more convenient, or more innovative products. They would especially find it less pressing to intensify their efforts to focus their R&D on the technological needs of the U.S. market specifically, deriving from the spectrum profile in the U.S. as well as its geography, demographics, and other characteristics. None of my analyses have quantified the cost to consumers of inferior network performance or depressed innovation that would be expected from excluding from the market the vendor that is the most technologically accomplished and that constitutes the most challenging technological competitor to the other vendors serving the United States.

CRA Charles River Associates

Debra J. Aron

Vice President

PhD, Economics
University of Chicago

BA, Economics
University of California at Los Angeles

Dr. Debra J. Aron is a Vice President in the Competition Practice. Debra applies her expertise in economic and policy matters, including competition and antitrust analysis, intellectual property, class certification, and damages analysis, in both regulatory and litigation disputes. She has provided expert testimony for over 20 years in a variety of high-stakes federal, state, regulatory, and arbitration cases relating to competition and antitrust including market definition, conduct cases, and price fixing damages, intellectual property damages including patents and trade secrets; class actions and class certification including consumer fraud matters and TCPA; pricing; unjust enrichment; and economic cost analyses. She also has conducted competition analyses in several high-profile mergers and macroeconomic analyses of pricing and investment changes. Dr. Aron's practice spans many industries, and she has a specific expertise in telecommunications and technology, including wireless services, wireline services, backbone, RAN, and customer premises equipment, satellite communications, and computer technology.

Publications

"Lessons from the Economic Deregulation of the Airline and Telecommunications Industries.," *Infrastructure* 58, no. 2 (Winter 2019).

"An Empirical Analysis of Regulator Mandates on the Pass Through of Switched Access Fees for In-State Long-Distance Telecommunications in the U.S.," with David E. Burnstein, Ana Danies, and Gerry Keith, June 19, 2013. Available at SSRN: http://ssrn.com/abstract=1674082.

Contributing author, ABA SECTION OF ANTITRUST LAW, TELECOM ANTITRUST HANDBOOK, Second Edition, (Chicago: American Bar Association), March 2013.

"The Effects of Legacy Pricing Regulation on Adoption of Broadband Service in the United States," with Allan T. Ingraham, *Review of Network Economics* 11, issue 4, 2012.

"Social Welfare Implications of Liability Rules in Major Environmental Damages Cases," with Francis X. Pampush, Environmental Litigation Committee Newsletter, Fall 2011.

"Regulatory Policy and the Reverse Cellophane Fallacy," with David E. Burnstein, *Journal of Competition Law and Economics* 2010; doi: 10.1093/joclec/nhp033.

"Investment in Next Generation Networks and Wholesale Telecommunications Regulation," with Robert W. Crandall, November 3, 2008. Available at SSRN: http://ssrn.com/abstract=1294910.

"Pricing Principles and Pricing Methodologies for Essential Facilities," May 2008.

Contributing author, ABA SECTION OF ANTITRUST LAW, TELECOM ANTITRUST HANDBOOK, (2005), (Chicago: American Bar Association), 2005.

"The Proper Treatment of Spare Network Capacity in Regulatory Cost Models," with Ana Danies, May 2005. Available at SSRN http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2133365.

"State Commissions Systematically Have Set UNE Prices Below Their Actual Costs," with Frank Pampush and E. Gerry Keith, November 2003. Available at SSRN http://ssrn.com/abstract=3327613.

"Broadband Adoption in the United States: An Empirical Analysis," with David E. Burnstein, in DOWN TO THE WIRE: STUDIES IN THE DIFFUSION AND REGULATION OF TELECOMMUNICATIONS TECHNOLOGIES, Allan Shampine, ed., (Nova Science Publishers, Hauppauge, NY, 2003).

"Developments in the Theory of Vertical Foreclosure as Applied to Regulated Telecommunications Markets" (March 2002), Prepared for Presentation at The American Bar Association Section of Antitrust Law, 50th Annual Spring Meeting.

"Modifications at HHIs for Vertical Supply Relationships" with Wenqing Li and James Langenfeld, White Paper submitted to European Commission, February 2000.

"Economic Theories of Tying and Foreclosure Applied—And Not Applied—in Microsoft," with Steven S. Wildman, *Antitrust* 14, no. 1, 1999, pp.48-52.

"Effecting a Price Squeeze Through Bundled Pricing," with Steven S. Wildman, in COMPETITION, REGULATION, AND CONVERGENCE: CURRENT TRENDS IN TELECOMMUNICATIONS POLICY RESEARCH, Gillett and Vogelsang, eds. (New Jersey: Lawrence Erlbaum Associates, Inc.) 1999, pp. 1-17.

"Worldwide Wait? How the Telecom Act's Unbundling Requirements Slow the Development of the Network Infrastructure," with Ken Dunmore and Frank Pampush, *Industrial and Corporate Change* 7, no. 4, 1998, pp. 615-621.

"The Pricing of Customer Access in Telecommunications," with Steven S. Wildman, *Industrial and Corporate Change* 5, no. 4, 1996, pp. 1029-1047.

"Bonus and Penalty Schemes as Equilibrium Incentive Devices, With Application to Manufacturing Systems," with Pau Olivella, *Journal of Law, Economics, and Organization* 10, Spring 1994, pp. 1-34.

"Diversification as a Strategic Preemptive Weapon," *Journal of Economics and Management Strategy* 2, Spring 1993, pp. 41-70.

"Using the Capital Market as a Monitor: Corporate Spin-offs in an Agency Framework," *RAND Journal of Economics* 22, Winter 1991, pp. 505-518.

"Firm Organization and the Economic Approach to Personnel Management, *American Economic Review* 80, no. 2, May 1990, pp. 23-27.

"The Introduction of New Products," with Edward P. Lazear, *American Economic Review* 80, no. 2, May 1990, pp. 421-426.

"Ability, Moral Hazard, Firm Size, and Diversification," *RAND Journal of Economics* 19, Spring 1988, pp. 72-87.

"Worker Reputation and Productivity Incentives," *Journal of Labor Economics* 5, no. 4, October 1987, part 2, pp. S87-S106.

"The Role of Managerial Ability and Moral Hazard in the Determination of Firm Size, Growth and Diversification," Ph.D. Dissertation, University of Chicago, August 1985.

Presentations

"Balancing Unquantified Benefits and Harms Under the Consumer Welfare Standard," The New York State Bar Association Antitrust Law Section, 2019 William Howard Taft Lecture, Commenter to the remarks of The Honorable Douglas H. Ginsburg, New York, New York, September 2019.

"The Impact on the U.S. Economy of Excluding Huawei from Participation in the U.S. Market for Wireless Network Equipment," Presentation at the Fiscal Year 2019 National Defense Authorization Act, Section 889, Public Meeting of Department of Defense, General Services Administration, and NASA, Washington DC, July 19, 2019.

Moderator, "Your Expert Is Your Friend: How to Effectively Deliver Expert Testimony," ABA: The Woman Advocate Committee Regional CLE Program: Raising the Bar, Chicago, IL, October 2018.

"Lessons from the Deregulation of the Airline and Telecommunications Industries," ABA Infrastructure and Regulated Industries Section, Dallas, Texas, August 2018.

"Economic Fundamentals: Vertical and Coordinated Effects in Mergers," ABA Section of Antitrust Law, Fundamentals of Antitrust Economics Series, Chicago, Illinois, July 2018.

Panelist, "Considerations for the Economists' Analysis in Opt-Out Relative to Class Action Litigation," ABA 5th Annual Western Regional CLE Program on Class Actions and Mass Torts, San Francisco, California, June 2018.

"Lessons from the Deregulation of the Airline and Telecommunications Industries," ABA Infrastructure and Regulated Industries Section, Fall Council Meeting, Palm Beach, Florida, October 2017.

"Economic Fundamentals: Vertical and Coordinated Effects in Mergers," ABA Section of Antitrust Law, Fundamentals of Antitrust Economics Series, Washington D.C., May 2016.

Panelist, "Economic Fundamentals: Market Power," ABA Spring Meeting, Washington D.C., April 2016.

"The Economic Impact of Electricity Price Increases in Puerto Rico," ABA Section of Public Utility, Communications and Transportation Law, Spring Council Meeting, Naples, FL, March 2016.

Moderator, "Effective Cross-Examination of the Expert Witness: Practical Tips and Video Clips," ABA Annual Meeting, Chicago, July 2015.

Moderator, "The Science of Persuasion: Practical Insights from Research on Expert Witness Effectiveness and Jury Decision-Making," ABA Section of Litigation Annual Conference, New Orleans, April 2015.

Panelist, "How to Manage Conversations with Expert Witnesses," ABA Section of Litigation, Environmental, Mass Torts, & Products Liability Litigation Committees' Joint CLE Seminar, Avon, Colorado, January 30, 2014.

"The Effects of Legacy Pricing Regulation on Adoption of Broadband Service in the United States," Federal Communications Commission, Washington, D.C., June 11, 2013.

Panelist, "A Primer: Getting the Most Out of Your Experts — Do's and Don'ts in the Use of Expert Witnesses: Learning from the Experts," ABA Section of Litigation Annual Conference, Chicago, Illinois, April 26, 2013.

"An Empirical Analysis of Regulator Mandates on the Pass Through of Switched Access Fees for In-State Long-Distance Telecommunications in the U.S.," with David E. Burnstein, Ana Danies, and Gerry Keith, Wesleyan University, Middletown, Connecticut, March 27, 2013.

"The Effects of Legacy Pricing Regulation on Adoption of Broadband Service in the United States," with Allan Ingraham, The 40th Research Conference on Communication, Information and Internet Policy (TPRC), September 22, 2012.

Panelist, "Two Decades of Daubert: Junk Science Replaced by Junk Rulings?" ABA Section of Litigation Annual Conference, Washington, DC, April 20, 2012.

"The Effects of Legacy Pricing Regulation on Adoption of Broadband Service in the United States," with Allan Ingraham, New America Foundation, workshop on Defining and Measuring Meaningful Broadband Adoption, April 11, 2012, Washington, DC.

"Social Welfare Implications of Liability Rules in Major Environmental Damages Cases," with Francis X. Pampush, American Bar Association Sections of Litigation and Criminal Justice Joint Annual Conference, April 15, 2011, Miami, Florida.

"Consumer Benefits of Intrastate Access Rate Reform in Minnesota," Center for Science, Technology and Public Policy, Humphrey School of Public Affairs, University of Minnesota, January 26, 2011.

"An Empirical Analysis of Regulator Mandates on the Pass Through of Switched Access Fees for In-State Long-Distance Telecommunications in the U.S.," with David E. Burnstein, Ana Danies, and Gerry Keith, The 38th Research Conference on Communication, Information and Internet Policy

Telecommunications Policy Research Conference), October 3, 2010, George Mason University Law School, Arlington, Virginia.

"Pricing Principles and Pricing Methodologies for Essential Facilities," The 36th Research Conference on Communication, Information and Internet Policy (TPRC), September 27, 2008.

"Regulatory Policy and the Reverse Cellophane Fallacy," with David E. Burnstein, 17th Biennial International Telecommunications Society Conference, Montréal, Québec, Canada, June 24-27, 2008.

"The Use of Economic Analysis in 'Industry Expert' Testimony," CLE course, XPRT Forum, March 7, 2008.

Presentations to the New Jersey Board of Public Utilities and to the New Jersey Legislature's Telecommunications Utilities Committee regarding the economic principles for a forward-looking regulatory agenda in light of the facts of competition nationwide and in New Jersey, and the costs of regulation, October – November 2006.

"The Interaction of Regulation with Economics and Financial Analysis in Litigation, Policy, and Strategy Consulting," CLE course, XPRT Forum, October 7, 2006.

"Comments on 'Economic Analysis in FCC Merger Proceedings,'" Conference on Economic Analysis and FCC Decisionmaking, presented by the Federal Communications Bar Association (FCBA) and Stanford Institute for Economic Policy Research (SIEPR), Washington D.C., March 15, 2006.

"Economic Principles for Consumer Protection Rules," Pri Telecom / Tech Briefing, Santa Clara, California, October 11, 2005.

"The Proper Treatment of Spare Network Capacity in Regulatory Cost Models," Presentation at the Advanced Workshop in Regulation and Competition, Center for Research in Regulated Industries, Skytop, Pennsylvania, May 2005.

"Telecommunications Regulation: What's Obsolete? What Will Become Obsolete?" Presentation at the State and City Telecom Reform Conference, Heartland Institute, Chicago, Illinois, December 2004.

"Trends in Telecommunications Demand & Supply," Presentation at the 46th Annual NARUC Regulatory Studies Program, Michigan State University, August 2004.

"The Economic Costs of Proposed Wireless Regulations in California," Presentation to Commissioners Brown and Kennedy, California Public Utilities Commission, San Francisco, California, April 2004.

"The Economics of UNE Pricing: Presentation to Staff," Ex parte presentation to the staff of the FCC, in FCC WC Docket No. 03-173: Review of the Commission's Rules Regarding the Pricing of Unbundled Network Elements and the Resale of Service by Incumbent Local Exchange Carriers,

March 2004.Unbundled Network Elements and the Resale of Service by Incumbent Local Exchange Carriers, March 2004.

“The High Cost of Proposed New Wireless Regulations,” Presentation to the Pacific Research Institute conference “Regulating Wireless in California: Bill of Rights... or Wrongs?,” San Francisco, April 2003.

“The TELRIC Showdown,” Panelist, NARUC Staff Subcommittee on Telecommunications, 2002 Annual Convention, Chicago, Illinois, November 2002.

“Economic Principles for Efficient Pricing of Municipal Rights-of-Way,” National Association of Telecommunications Officers and Advisors (NATOA), Chicago, Illinois, September 2002.

“Trends in Voice and Broadband Competition in Telecommunications Markets: Markets, Strategies, and Regulation,” 82nd Annual Convention of the Indiana Telecommunications Association, Lexington, Kentucky, June 2002.

“Broadband Deployment in the United States,” Emerging Opportunities in Broadband Symposium, Northwestern University, Evanston, Illinois, December 2001.

“Local Competition in Illinois,” Illinois Telecommunications Symposium, Northwestern University, Evanston, Illinois, December 2000.

“Licensing and Access to Innovations in Telecommunications and Information Services,” Telecommunications Policy Research Conference, Alexandria, Virginia, September 2000.

“Effecting a Price Squeeze Through Bundled Pricing,” Federal Communications Commission, Washington, D.C., May 1999.

“Competitive and Strategic Use of Optional Calling Plans and Volume Pricing Plans,” The Institute for International Research Conference for Competitive Pricing of Telecommunications Services, Chicago, Illinois, July 1998.

“Effecting a Price Squeeze Through Bundled Pricing,” Consortium for Research in Telecommunications Policy Conference, University of Michigan, Ann Arbor, Michigan, June 1998.

“The Pricing of Customer Access in Telecommunications,” Conference on Public Policy and Corporate Strategy for the Information Economy, Evanston, Illinois, May 1996.

“Diversification as a Strategic Preemptive Weapon,” University of Iowa, Iowa City, Iowa, February 1994.

"Diversification as a Strategic Preemptive Weapon, "University of Buffalo, Buffalo, New York, February 1994.

"Diversification as a Strategic Preemptive Weapon," University of Southern California, Los Angeles, California, December 1993.

"Strategic Pricing," Winter Meetings of the Econometric Society, Discussant, Anaheim, California, December 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Michigan State University, Lansing, Michigan, November 1993.

"Diversification as a Strategic Preemptive Weapon," Rutgers University, New Brunswick, New Jersey, November 1993.

"Diversification as a Strategic Preemptive Weapon," University of California at Santa Cruz, Santa Cruz, California, November 1993.

"Diversification as a Strategic Preemptive Weapon," Graduate School of Business, Stanford University, Stanford, California, November 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Purdue University, West Lafayette, Indiana, September 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Summer Meetings of the Econometric Society, Boston University, Boston, Massachusetts, June 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," University of California, Department of Economics, Berkeley, California, May 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Stanford University, Graduate School of Business, Stanford, California, May 1993.

"Diversification as a Strategic Preemptive Weapon," Stanford University, Graduate School of Business, Stanford, California, April 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Hoover Institution, Stanford, California, April 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets,"

University of California, Graduate School of Business, Berkeley, California, February 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Stanford University, Department of Economics, Stanford, California, February 1993.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," Hoover Institution, Stanford, California, January 1993.

"Pricing Strategies," Session Discussant, 1992 North American Winter Meeting of The Econometric Society, Anaheim, California, January 1992.

"Diversification as a Strategic Preemptive Weapon," University of Toronto, Toronto, Canada, November 1991.

"Diversification as a Strategic Preemptive Weapon," Queen's University, Kingston, Ontario, Canada, November 1991.

"Bonuses and Penalties as Equilibrium Incentive Devices, with Application to Manufacturing Systems," University of Chicago, Chicago, Illinois, June 1991.

"The Timing of Entry into New Markets," Summer Meetings of the Econometric Society, University of Pennsylvania, Philadelphia, Pennsylvania, June 1991.

"Innovation, Imitation, Productive Differentiation, and the Value of Information in New Markets," University of Chicago, Chicago, Illinois, April 1991.

"Bonuses and Penalties as Equilibrium Incentive Devices, with Application to Manufacturing Systems," Winter Meetings of the Econometric Society, Washington, D.C., December 1990.

"Corporate Spin-offs in an Agency Framework," University of Washington, Seattle, Washington, October 1990.

"The Timing of Entry Into New Markets," University of British Columbia, Vancouver, British Columbia, October 1990.

"Corporate Spin-offs in an Agency Framework," Texas A&M University, College Station, Texas, April 1990.

"Firm Organization and the Economic Approach to Personnel Management," Winter Meetings of the American Economic Association, New York, New York, December 1989.

"Corporate Spin-offs in an Agency Framework," Western Finance Association Meetings, Seattle, Washington, June 1989.

"Corporate Spin-offs in an Agency Framework," University of Rochester, Rochester, New York, May 1989.

"Corporate Spin-offs in an Agency Framework," North American Summer Meetings of the Econometric Society, Minneapolis, Minnesota, June 1988.

"Competition, Relativism, and Market Choice," North American Summer Meetings of the Econometric Society, Berkeley, California, June 1987.

"Competition, Relativism, and Market Choice," University of Chicago, Chicago, Illinois, April 1987.

"Rate Reform and Competition in Electric Power," Discussant, Conference on Competitive Issues in Electric Power, Northwestern University, Evanston, Illinois, March 1987.

"Worker Reputation and Productivity Incentives," New Economics of Personnel Conference, Arizona State University, Tempe, Arizona, April 1986.

"Ability, Moral Hazard, and Firm Diversification," Various Universities, 1985, 1994, including Yale University, University of Rochester, Stanford University, University of Minnesota, California Institute of Technology, Duke University, Northwestern University, Brown University, Harvard University, University of California - Los Angeles, University of Pennsylvania.

Academic Journal Refereeing

Dr. Aron has served as a referee for The Rand Journal of Economics, the Journal of Political Economy, the Journal of Finance, the American Economic Review, the Quarterly Journal of Economics, the Journal of Industrial Economics, the Journal of Economics and Business, the Journal of Economic Theory, the Journal of Labor Economics, the Review of Industrial Organization, the European Economic Review, the Journal of Economics and Management Strategy, the International Review of Economics and Business, the Quarterly Review of Economics and Business, Management Science, the Journal of Public Economics, the Journal of Institutional and Theoretical Economics, and the National Science Foundation.

Testimony (2011-2019)

Deposition of Debra J. Aron in Motorola Solutions, Inc. et al. v. Hytera Communications Corporation Ltd. et al., United States District Court, for the Northern District of Illinois, Eastern Division, Case No. 1:17-cv-01973, September 20, 2019.

Deposition of Debra J. Aron in Jonathan Coffey et al. v. WCW & Air, Inc. et al., United States District Court, for the Northern District of Florida, Pensacola Division, Case No. 3:17-cv-90-TKW-HTC, September 13, 2019.

Deposition of Debra J. Aron in Sumotext Corp. v. Zoove, Inc. et al., United States District Court, Northern District of California, San Jose Division, Case No. 5:16-cv-01370-BLF-NMCx, August 1, 2019.

Deposition of Debra J. Aron in Waddell Williams, et al. v. Bluestem Brands, Inc., United States District Court, Middle District of Florida, Tampa Division, Case No. 8:17-CV-1971-T-27AAS, September 21, 2018.

Deposition of Debra J. Aron in Robert Hossfeld, et al. v. Compass Bank, N.A., et al., United States District Court, Northern District of Alabama, Southern Division, Case No. 2:16-CV-2017-ACA, September 7, 2018.

Deposition of Debra J. Aron in Ventures Edge legal, PLLC, et al. v. GoDaddy.com, LLC, et al., United States District Court, District of Arizona, Case No. 2:15-cv-02291-GMS, January 30, 2018.

Deposition of Debra J. Aron in Rajesh Verma, et al. v. Memorial Healthcare Group Inc., et al., United States District Court, Middle District of Florida, Jacksonville Division, Case No. 3:16-CV-00427-HLA-JRK, June 27, 2017.

Trial Testimony of Debra J. Aron in T-Mobile USA, Inc. v. Huawei Device, USA, Inc., et al., In the United States District Court for the Western District of Washington at Seattle, Case No. C14-1351-RAJ, May 12, 2017.

Deposition of Debra J. Aron in Re Optical Disk Drive Antitrust Litigation, Hewlett-Packard Company v. Toshiba Corp., et al., United States District Court, Northern District of California, MDL Docket No. 3:10-MD-02143-RS, Case No. 3:13-cv-05370-RS, March 23, 2017.

Deposition of Debra J. Aron in Peerless Network, Inc., et al. v. AT&T Corp., In the United States District Court for the Southern District of New York, Case No. 15 CV 870, February 17, 2017.

Trial Testimony of Debra J. Aron in Thomas H. Krakauer, et al. v. Dish Network, L.L.C., In the United States District Court for the Middle District of North Carolina, Durham Division, Case No.

1:14-CV-333, January 17, 2017.

Deposition of Debra J. Aron in T-Mobile USA, Inc. v. Huawei Device, USA, Inc., et al., In the United States District Court for the Western District of Washington at Seattle, Case No. C14-1351-RAJ, September 29, 2016.

Deposition of Debra J. Aron in Southwestern Bell Telephone Co., et al. v. V247 Telecom, LLC, et al., In the United States District Court for the Northern District of Texas, Dallas Division, Case No. 3:14-CV-01409-M, August 31, 2016.

Hearing Testimony of Dr. Debra J. Aron in Order Instituting Investigation into the State of Competition Among Telecommunications Providers in California, and to Consider and Resolve Questions raised in the Limited Rehearing of Decision 08-09-042, Before the Public Utilities Commission of the State of California, Investigation 15-11-007, July 20, 2016.

Prefiled Written Rebuttal Testimony of Dr. Debra J. Aron in Order Instituting Investigation into the State of Competition Among Telecommunications Providers in California, and to Consider and Resolve Questions raised in the Limited Rehearing of Decision 08-09-042, Before the Public Utilities Commission of the State of California, Investigation 15-11-007, July 15, 2016.

Prefiled Written Testimony of Dr. Debra J. Aron in Order Instituting Investigation into the State of Competition Among Telecommunications Providers in California, and to Consider and Resolve Questions raised in the Limited Rehearing of Decision 08-09-042, Before the Public Utilities Commission of the State of California, Investigation 15-11-007, June 1, 2016 and March 5, 2016.

Deposition of Debra J. Aron in Ramzy Ayyad, et al. v. Sprint Spectrum, L.P., In the Superior Court of the State of California for the County of Alameda, Case No.: RG03-121510, March 29, 2016.

Deposition of Debra J. Aron in Avnet, Inc. and BSP Software, LLC v. Motio, Inc., In the United States District Court for the Northern District of Illinois, Eastern Division, Case No.: 1:12-cv-2100, March 9, 2016.

Deposition of Debra J. Aron in Lena K. Thodos and David Miller, et al. v. Nicor, Inc., et al., In the Circuit Court of Cook County, Illinois County Department, Chancery Division, Case No.: 1:12-cv-2100, February 22, 2016.

Deposition of Debra J. Aron in Henry Espejo v. Santander Consumer USA, Inc., In the United States District Court for the Northern District of Illinois, Eastern Division, Case No.: 1:11-cv-08987, January 12, 2016.

Deposition of Debra J. Aron in Rachel Johnson, et al., v. Yahoo!, Inc. and Zenaida Calderin, et al. v. Yahoo!, Inc., in the United States District Court for the Northern District of Illinois, Eastern Division,

Case Nos.: 14-cv-2028 and 14-cv-2753 and Rafael David Sherman, et al., v. Yahoo!, Inc., In the United States District Court for the Southern District of California, Case No.: 13-CV-00041-GPC-WVG (Combined), June 23, 2015.

Trial Testimony of Debra J. Aron in Salsgiver Communications, Inc., et al., v. Consolidated Communications Holdings, Inc., et al., In the Court of Common Pleas, Allegheny County, Pennsylvania, Case No. No. GD 08-7616, May 2015.Communications Holdings, Inc., et al., In the Court of Common Pleas, Allegheny County, Pennsylvania, Case No. No. GD 08-7616, May 2015.

Deposition of Debra J. Aron in Herbert Chen et al. v. Robert Howard-Anderson et al., In the Court of Chancery of the State of Delaware, Case No. C.A. 5878-VCL, December 16, 2014.

Deposition of Debra J. Aron in Sprint Communications Company L.P. v. Comcast Cable Communications, LLC, et al., In the United States District Court for the District of Delaware, Case No. 1:12-cv-01013-RGA, November 20, 2014.

Testimony of Debra J. Aron in Bayer CropScience LP v. Albaugh, Inc., et al., Before the American Arbitration Association, Case No. 16-171-Y-00511-12, October 20-21, 2014.

Trial Testimony of Debra J. Aron in Comcast IP Holdings I, LLC v. Sprint Communications Company L.P., et al., In the United States District Court for the District of Delaware, Case No. 12-205-RGA (CJB), October 9, 2014.

Prefiled Written Reply Testimony of Debra J. Aron in The Utility Reform Network v. Pacific Bell Telephone Company, Before the Public Utilities Commission of the State of California, Case No. 13-12-005, October 3, 2014.

Deposition of Debra J. Aron in Amanda Balschmiter, et al., v. TD Auto Finance, LLC, In the United States District Court, Northern District of Illinois, Eastern Division, Case No. 13cv1186, September 10, 2014.

Prefiled Written Testimony of Debra J. Aron in The Utility Reform Network v. Pacific Bell Telephone Company, Before the Public Utilities Commission of the State of California, Case No. 13-12-005, August 22, 2014.

Deposition of Debra J. Aron in Grant Birchmeier, et al., v. Caribbean Cruise Line, Inc., et al., In the United States District Court, Northern District of Illinois, Eastern Division, Case No. 12 CV 4069, July 19, 2014.

Deposition of Debra J. Aron in Comcast IP Holdings I, LLC v. Sprint Communications Company L.P., et al., United States District Court for the District of Delaware, Case No. 12-205-RGA(CJB), July 11, 2014.

Deposition of Debra J. Aron in In re: Methyl Tertiary Butyl Ether Products Liability Litigation, Commonwealth of Puerto Rico, et al., v. Shell Oil Co., et al., In the United States District Court, Southern District of New York, Case No. 07 Civ. 10470, May 27, 2014.

Depositions of Debra J. Aron in In re: Polyurethane Foam Antitrust Litigation, General Motors, L.L.C. v. Carpenter Co., et al., In the United States District Court for the Northern District of Ohio, Western Division, Case No. 3:12-pf-10027-JZ, April 30, 2014 and September 8, 2014.

Trial Testimony of Debra J. Aron in Seth Warnick, et al., v. Dish Network, L.L.C., In the United States District Court, District of Colorado, Civil Action No. 12-cv-01952-WYD, March 20, 2014.

Deposition of Debra J. Aron in Seth Warnick, et al., v. Dish Network, L.L.C., In the United States District Court, District of Colorado, Civil Action No. 12-cv-01952-WYD, September 25, 2013.

Deposition of Debra J. Aron in In re: Methyl Tertiary Butyl Ether ("MTBE") Product Liability Litigation, New Jersey Department of Environmental Protection, et al. v. Atlantic Richfield Co., et al., In the United States District Court, Southern District of New York, No. 08 Civ. 312, May 29, 2013.

Prefiled Written Testimony and Reply Testimony of Debra J. Aron in In the Matter of the Petition Filed by ALASCOM, INC. d/b/a AT&T ALASKA to be Relieved of its Carrier of Last Resort Responsibilities in Certain Locations in Southwest Alaska, Before the Regulatory Commission of Alaska, Docket No. U-12-127, April 1, 2013 and January 17, 2013.

Deposition of Debra J. Aron in William Douglas Fulghum, et al., v. Embarq Corporation, et al., In the United States District Court for the District of Kansas, Civil Action No.: 07-CV-2602 (EFM/JPO), November 29, 2011.

Deposition of Debra J. Aron in Southwestern Bell Telephone Company, et al., v. IDT Telecom, Inc., et al., In the United States District Court, Northern District of Texas, Dallas Division, Civil Action No. 3-09-CV-1268-P, November 10, 2011.

Direct and Rebuttal Testimony of Debra J. Aron in the Matter of Petition of Sprint to Reduce Intrastate Switched Access Rates of Incumbent Local Exchange Carriers in North Carolina, Before the North Carolina Utilities Commission, Docket No. P-100, Sub 167, August 18, 2011 and September 27, 2011.

Prefiled Written Testimony and Rebuttal Testimony of Debra J. Aron in the Matter of: An Investigation Into the Intrastate Switched Access Rates of All Kentucky Incumbent and Competitive Local Exchange Carriers, Commonwealth of Kentucky, Before the Public Service Commission, Docket No. 2010-00398, September 30, 2011, and July 8, 2011.

Testimony of Debra J. Aron before the Utilities Committee of the Kansas Legislature regarding the

status of competition in telecommunications markets in Kansas, February 2011.

Testimony of Debra J. Aron before the Telecommunications Committee of the Legislature of the state of Washington regarding the consumer benefits and competitive effects of switched access reform, February 2011.

Professional organizations

Member, American Economic Association

Member, Econometric Society

Associate Member, American Bar Association

Past Member, Telecommunications Policy Research Conference Program Committee

Honors and awards

Guthman Research Chair, Kellogg Graduate School of Management, Northwestern University, Summer 1994.

Hoover National Fellowship, Hoover Institution, 1992-1993.

Faculty Research Fellow, National Bureau of Economic Research, 1987-1990.

PepsiCo Research Chair, Northwestern University, 1990.

Kellogg Research Professorship, Northwestern University, 1989.

National Science Foundation Research Grant, 1987-1988.

Buchanan Chair, Kellogg Graduate School of Management, Northwestern University, 1987-1988.

IBM Chair, Kellogg Graduate School of Management, Northwestern University, 1986-1987.

Teaching

Courses taught: Pricing Strategy; Information, Communication, and Competition (economics of strategy and competition); Intermediate Microeconomic Theory; Managerial Economics (microeconomic theory as applied to business strategy and decision making) at the M.B.A. level, The Economics of Information at the Ph.D. level.

Also qualified to teach: graduate Microeconomic Theory; Industrial Organization and Labor Economics; the Economics of Personnel; Public Finance; Project Evaluation; Applied Game Theory.

Professional history

2019–Present	*Vice President*, Charles River Associates, Chicago, IL
2018–2019	*Principal and Senior Managing Director*, Ankura Consulting Group, Chicago, IL
2010-2018	*Principal and Managing Director*, Navigant Economics, Chicago, IL
2000-2016	*Adjunct Associate Professor*, Northwestern University, Evanston, IL
1995-2010	*Managing Director*, LECG, LLC, Evanston, IL
1993-1995	*Visiting Assistant Professor of Managerial Economics*, Northwestern University, Evanston, IL
1985-1992	*Assistant Professor of Managerial Economics*, Northwestern University, Evanston, IL
1992-1993	*National Fellow*, Hoover Institution at Stanford University, Stanford, CA
1983-1984	*Instructor*, University of Chicago Department of Economics, Chicago, IL
1979-1980	*Staff Economist*, Civil Aeronautics Board, Office of Economic Analysis, Washington, D.C.

October 2019

APPENDICES

Table of Contents

A. PROFILES OF THE MAJOR RAN EQUIPMENT PROVIDERS 1
- i. Huawei 1
- ii. Ericsson 2
- iii. Nokia 3
- iv. Samsung 4
- v. ZTE 4

B. ESTIMATE OF THE IMPACT OF THE PENETRATION RATE OF NEW WIRELESS TECHNOLOGY GENERATION ON GDP PER CAPITA 5
- i. Estimate of the Relationship Between Delay in 5G Deployment and Delay in 5G Adoption 11

C. CALCULATION OF THE EFFECT ON EQUIPMENT VENDOR PRICES OF EXCLUDING HUAWEI FROM SALES OF RAN NETWORK EQUIPMENT IN THE UNITED STATES 14

D. STATE OF 5G DEPLOYMENTS IN THE UNITED STATES AND OTHER COUNTRIES 19
- i. United States 19
- ii. Australia 21
- iii. China 22
- iv. Japan 22
- v. South Korea 23
- vi. Switzerland 23
- vii. United Kingdom 24
- viii. United Arab Emirates 25

A. PROFILES OF THE MAJOR RAN EQUIPMENT PROVIDERS

i. Huawei

1. Huawei Technologies Co., Ltd. ("Huawei") is a wholly-owned subsidiary of Huawei Investment & Holding Co., Ltd. ("Huawei Group"), headquartered in Shenzhen in the People's Republic of China.[1] Huawei Group operates in many different facets of the communications industry, from designing and manufacturing wired and wireless communication infrastructure equipment to developing, testing, and producing smartphones.[2] I understand that Huawei is responsible for "development, manufacture and sale of telecommunication and related products and provision of support and maintenance services."[3]

2. Huawei Group has historically operated in China since its founding in 1987; however, it has expanded into international markets in recent years.[4]

3. Huawei Group conducts business in three operating segments: 1) Carrier Business, 2) Enterprise Business, and 3) Consumer Business.[5] Huawei Group's Carrier Business segment designs, manufactures and sells fixed and wireless network equipment, and related software, among other products.[6] This segment provides services to global telecommunications carriers, including services such as simplified operations and maintenance of 5G networks, cloud-network convergence services, and network rollout services.[7]

4. Huawei Group's Enterprise Business segment develops information and communications technology (abbreviated as "ICT") products and solutions by using, for example, cloud

---

[1] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, pp. 74, 123.
[2] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, pp. 97, 123.
[3] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 123.
[4] Edwin Chan, "Huawei's Profit Jumps as It Makes Headway Beyond China," *Bloomberg Technology*, Updated April 1, 2016, at http://www.bloomberg.com/news/articles/2016-04-01/huawei-s-profit-jumps-as-it-makes-headway-beyond-slowing-china.
[5] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 97.
[6] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, pp. 97, 123.
[7] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, pp. 21 and 97.

computing, big data and Internet of Things ("IoT"), and software-defined networking.[8] Huawei Group provides these solutions to customers in various industries including governments, public utilities, energy, transport manufacturing, and finance.[9] Huawei Group's Consumer Business segment develops, manufactures, and sells smartphones, tablets, wearable devices, converged home devices, and applications for these devices for consumers and businesses.[10]

5. Huawei Group generated approximately $107 billion in revenue in 2018. The Carrier segment accounted for approximately 41 percent of total revenues, the Enterprise segment accounted for approximately 10 percent of revenues, the Consumer segment accounted for approximately 48 percent of revenues, and the rest was specified as unallocated revenue.[11]

ii. Ericsson

6. Ericsson is a publicly-owned company headquartered in Stockholm, Sweden.[12] Ericsson divides its market activities into four segments: Networks, Digital Services, Managed Services, and Emerging Business and Other.[13] The Networks segment provides hardware, software, and services to carriers to build and evolve their mobile networks; Digital Services provides software to customers to operate and monetize their mobile networks; Managed Services provides services related to network operations; and Emerging Business and Other offers new innovative services such as Internet of Things.[14] Ericsson has three wholly-owned subsidiaries in China. Ericsson also has a joint venture with Nanjing Panda Electronics, Nanjing Ericsson Panda Communication Co., Ltd. Nanjing Panda Electronics is partially owned by the Chinese government.[15] In addition, some of Ericsson's

[8] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, pp. 97, 153.
[9] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, p. 97.
[10] Huawei Investment & Holding Co., Ltd., 2018 Annual Report, pp. 97, 123.
[11] "Huawei Investment Holding Co., Ltd., Financials" S&P Capital IQ.
[12] Telefonaktiebolaget LM Ericsson, 2018 Annual Report, pp. 133, 205.
[13] Telefonaktiebolaget LM Ericsson, 2018 Annual Report, p. 9.
[14] Telefonaktiebolaget LM Ericsson, 2018 Annual Report, p. 9.
[15] Telefonaktiebolaget LM Ericsson, 2018 Annual Report, pp. 107-108; "Investor Relations: Ownership," Panda Electronics Group, Co., Ltd., at http://www.panda.cn/gqjg/index_393.aspx.

production sites are in China.[16] Ericsson's total revenue in 2018 was approximately $23 billion.[17]

iii. Nokia

7. Nokia is a public company incorporated and domiciled in Helsinki, Finland.[18] Nokia's business is organized into seven groups: Mobile Networks, Fixed Networks, Global Services, IP/Optical Networks, Nokia Software, Nokia Enterprise (these six groups together constitute "Networks business"), and Nokia Technologies.[19] Mobile Networks provides technology for mobile access and microwave transport ranging from 2G to 5G;[20] Fixed Networks serves carriers and provides copper, cable, fiber, fixed wireless access, and Wi-Fi technologies;[21] Global Services provides services for mobile networks and managed services for the fixed, mobile, applications, IP, and optical domains;[22] IP/Optical Networks provides routing and optical technologies to carriers;[23] Nokia Software provides software to carriers and large enterprises to monetize, automate, make more intelligent, and/or upgrade networks;[24] Nokia Enterprise provides services related to the implementation and management of enterprise networks;[25] and Nokia Technologies focuses on the licensing of Nokia intellectual property, including patents, technologies, and the Nokia brand, and managing patent portfolio.[26] Nokia has a China-based joint venture called Nokia Shanghai Bell. Nokia holds 50 percent of shares plus one share ownership in Nokia Shanghai Bell's parent company, Nokia Shanghai Bell Co., Ltd. All other shares of Nokia Shanghai Bell Co., Ltd. are owned by the state-controlled China Huaxin.[27] Nokia also has one of its

[16] Telefonaktiebolaget LM Ericsson, 2018 Annual Report, p. 40.
[17] Telefonaktiebolaget LM Ericsson, Available: S&P Capital IQ, McGraw Hill Financial.
[18] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 136.
[19] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 3.
[20] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 12.
[21] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 14.
[22] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 16.
[23] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 18.
[24] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 20.
[25] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 22.
[26] Nokia Corporation, Form 20-F, for the fiscal year ended December 31, 2018, p. 24.
[27] Nokia Corporation, 2018 Annual Report, pp. 170-171.

manufacturing sites located in China.[28] Nokia's revenue was approximately $25 billion in 2018.[29]

iv. Samsung

8. Samsung is headquartered in Suwon, the Republic of Korea.[30] Samsung and its subsidiaries operate the following four segments: Consumer Electronics, Information Technology & Mobile communications, Device Solutions, and Harman. The Consumer Electronics segments includes digital TVs, monitors, air conditioners, and refrigerators; the Information Technology & Mobile communications includes mobile phones, communications systems, and computers; Device Solutions includes products such as memory, foundry and system LSI in the semiconductor business and LCD and OLED panels in the display business; and Harman includes connected car systems, visual products, audio products, enterprise automation solutions, and connected services.[31] Samsung has numerous subsidiaries in China, including R&D centers and manufacturing facilities.[32] Samsung is the biggest seller of wireless handsets worldwide.[33] Samsung's revenue was approximately $214 billion in 2018.[34]

v. ZTE

9. ZTE is based in Shenzhen, China.[35] ZTE's business is divided into three segments: carriers' network, government and corporate business, and consumer business. ZTE offers wireless products including base stations, network optimization tools, controllers, network

---

[28] Nokia Corporation, 2018 Annual Report, p. 108.

[29] Nokia Corporation, Available: S&P Capital IQ, McGraw Hill Financial.

[30] "Company Overview of Samsung Electronics Holding Co., Ltd.," Bloomberg L.P., at https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=91868.

[31] "Consolidated Financial Statements of Samsung Electronics Co., LTD. and Its Subsidiaries. Index to Financial Statements," p. 14.

[32] "Consolidated Financial Statements of Samsung Electronics Co., LTD. and Its Subsidiaries. Index to Financial Statements," Notes to the Consolidated Financial Statements, pp. 18-24.

[33] "Smartphone Shipments Experience Deeper Decline in Q1 2019 with a Clear Shakeup Among the Market Leaders, According to IDC," *IDC Corporate USA*, April 30, 2019, at https://www.idc.com/getdoc.jsp?containerId=prUS45042319.

[34] "Samsung Electronics Co., Ltd. KOSE A005930 Financials," S&P Capital IQ.

[35] "About Us," ZTE USA, at https://www.zteusa.com/about-us-old.

management products, and wireless infrastructure products. It also provides cloud computing and cloud infrastructure products, home media center products, and handsets.[36]

10. ZTE's revenue in 2018 was approximately $12.7 billion, approximately 64 percent of which came from its domestic market.[37] Carriers' networks revenue accounted for approximately 67 percent of ZTE's 2018 revenue, consumer business revenue accounted for approximately 22 percent, and government and corporate business accounted for approximately 11 percent.[38]

B. ESTIMATE OF THE IMPACT OF THE PENETRATION RATE OF NEW WIRELESS TECHNOLOGY GENERATION ON GDP PER CAPITA

11. To quantify the impact of the penetration rate of new wireless technology generation on GDP per capita I estimate the following regression model:

$$\begin{aligned}\ln(GDP\ per\ Capita_{it}) &= \alpha_0 + \alpha_1 * \ln(GDP\ per\ Capita_{it-1}) + \alpha_2 \\ &* \ln(GDP\ per\ Capita_{it-2}) + \alpha_3 * 4G\ Penetration\ Rate_{it} \\ &+ \alpha_4 * Mobile\ Penetration\ \mathrm{Rate}_{it} + \alpha_5 \\ &* Trade\ (\%\ of\ GDP)_{it} + \alpha_6 * Investment\ (\%\ of\ GDP)_{it} \\ &+ \alpha_7 * \ln(Labor_{it}) + \epsilon_{it}\end{aligned} \tag{1}$$

where $GDP\ per\ Capita_{it}$ is GDP per capita in 2010 USD at time t in country i; 4G $Penetration\ Rate_{it}$ is the penetration rate of 4G in country i at time t;[39] $Mobile\ Penetration\ Rate_{it}$ is the overall penetration rate of mobile phones (of any technology) in country i at time t; $Trade\ (\%\ of\ GDP)_{it}$ is the sum of exports and imports of goods and services as a share of GDP in country i at time t; $Investment\ (\%\ of\ GDP)_{it}$ is the net investment in nonfinancial assets measured as a share of GDP in country i at time t; $Labor_{it}$ is the total supply of labor in country i at time t; $\alpha_0, \ldots, \alpha_7$ are the regression

[36] See "Company Overview of ZTE Corporation," Bloomberg L. P., at https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=3051118; Annual Report, ZTE Corporation, 2018 (hereafter, *2018 ZTE Annual Report*), p. 31.

[37] *2018 ZTE Annual Report*, p. 31.

[38] ZTE Corporation, Available: S&P Capital IQ, McGraw Hill Financial.

[39] The 4G penetration rate in a country is calculated as the number of 4G-capable mobile devices in a country divided by the total population of that country.

coefficients to be estimated; and ϵ_{it} is the regression error term that captures idiosyncratic factors in country i at time t that are not captured by the explanatory variables in the regression.

12. The coefficient of interest is α_3. A positive and significant estimate of α_3 is consistent with the conclusion that a higher 4G penetration rate results in a higher GDP per capita. The estimated coefficient is the estimated percentage effect on GDP per capita of an increase in the 4G penetration rate of one percentage point.

13. I examine data from GSMA Intelligence on 4G penetration rates and mobile penetration rates in Australia, Canada, China, Germany, Japan, South Korea, the United States, and the United Kingdom. Data on GDP per capita, investment, labor force, and trade are taken from the World Bank's World Development Indicators ("WDI") database.[40] I exclude China from the regression sample because many observations are missing for this country in the WDI database.

14. The regression equation (1) might suffer from endogeneity. Endogeneity arises when there is a reverse causality issue or omitted variable bias. A reverse causality issue arises when there is a causal relationship between the outcome variable (e.g., GDP per capita) and an independent variable (e.g., the 4G penetration rate) in both directions. An omitted variable bias exists when there is a variable that is not included in the regression model but that affects both the outcome variable and one or several independent variables. For example, if certain government regulations have an effect on both GDP per capita and the 4G penetration rate, then the estimated effect of the 4G penetration rate on GDP per capita may be biased.

[40] See "Databank. World Development Indicators," the World Bank, at https://databank.worldbank.org/data/source/world-development-indicators.

15. My regression equation follows the regression specification estimated by Deloitte in its 2012 report.[41] Similar to the estimation strategy in Deloitte's report, I use the Arellano-Bond estimator to account for both types of endogeneity.[42] I apply the one-step Arellano-Bond estimator with 4G penetration rate and mobile penetration rate as contemporaneously endogenous variables and labor, investment, and trade as predetermined variables.[43] Exhibit B.1 shows the results.

---

[41] "What is the impact of mobile telephony on economic growth? A Report for the GSM Association." Deloitte, November 2012, pp. 13-14. Unlike the Deloitte study, I do not include government expenditures in my model because including this variable results in the violation of the critical assumption for Arellano-Bond estimator that the regression error terms are serially uncorrelated. See A. Colin Cameron and Pravin K. Trivedi, MICROECONOMETRICS USING STATA, Revised ed. (College Station, TX: StataCorp LP, 2010), p. 300.

[42] A. Colin Cameron and Pravin K. Trivedi, MICROECONOMETRICS USING STATA, Revised ed. (College Station, TX: StataCorp LP, 2010), pp. 293-301.

[43] Predetermined regressors are regressors that are correlated with past errors and are uncorrelated with present or future errors. Contemporaneously endogenous regressors are regressors that are correlated with past and present errors and are uncorrelated with future errors. See A. Colin Cameron and Pravin K. Trivedi, MICROECONOMETRICS USING STATA, Revised ed. (College Station, TX: StataCorp LP, 2010), p. 295.

Exhibit B.1
Regression Results for the Estimate of the Impact of the 4G Penetration Rate on GDP per Capita. Arellano-Bond Estimator, 2012-2017

	(1) $\ln(\text{GDP per Capita}_t)$	(2) $\ln(\text{GDP per Capita}_t)$
$\ln(\text{GDP per Capita})_{t-1}$	0.207	0.503**
	(0.132)	(0.213)
$\ln(\text{GDP per Capita})_{t-2}$	0.073	0.022
	(0.059)	(0.081)
Investment (% of GDP)$_t$	−0.013**	
	(0.006)	
Trade (% of GDP)$_t$	−0.001***	−0.001***
	(0.000)	(0.000)
$\ln(\text{Labor})_t$	0.182**	0.031
	(0.083)	(0.144)
4G Penetration Rate$_t$	0.043***	0.035**
	(0.014)	(0.017)
Mobile Penetration Rate$_t$	0.030*	0.021
	(0.018)	(0.015)
Observations	36	42

Notes:
[1] Models (1) and (2) are estimated using one-step Arellano-Bond estimator. 4G penetration rate and mobile penetration rate are assumed to be contemporaneously endogenous; trade, investment, and labor are assumed to be pre-determined.
[2] Robust standard errors are in parentheses.
[3] *significant at 90% level; **significant at 95% level; and ***significant at 99% level.

Sources:
[1] "DataBank. World Development Indicators," The World Bank, Series "GDP per capita (constant 2010 US$)," "Trade (% of GDP)," "Net investment in nonfinancial assets (% of GDP)," "Labor force, total," at https://databank.worldbank.org/data/source/world-development-indicators.
[2] GSMA Intelligence 2019 mobile subscriptions and statistics reports for Australia, Canada, Germany, Japan, South Korea, the U.K., and the U.S.

16. I run two regression models: Model (1) uses all variables from equation (1); Model (2) uses all variables from equation (1) but excludes net investment as a share of GDP, because this variable is missing for all counties in 2017, except for Canada. The results of the two models are similar. Model (1) indicates that when the 4G penetration rate increases by 1 percentage point, GDP per capita increases by 0.043 percent. Model (2) indicates that when the 4G penetration rate increases by 1 percentage point, GDP per capita increases by 0.035 percent. In my estimate of the impact of 5G adoption delay, I use the more conservative result of Model (2).

17. To ensure the validity of my estimates, I perform two specification tests of my estimator. I run the Arellano-Bond test for zero autocorrelation (i.e., no serial correlation in an error

term is a key assumption of the Arellano-Bond estimator). I also run the Sargan test for overidentifying restrictions.[44] Both tests do not reject the null hypothesis at a 95 percent confidence level that the model assumptions are met.

18. Exhibit B.2 shows my calculations of the cost of delay in 5G penetration rate on U.S. GDP for delay durations of 6, 12, 18, and 24 months. To calculate the incremental cost of the delay associated with the absence of Huawei, I subtract the cost of delay resulting from the spectrum gap—6 month delay—from the estimated cost associated with delay durations equal to 12, 18, and 24 months. Exhibit VIII.1 shows that the estimated cost of delay resulting from the Huawei ban ranges from approximately $104 billion to $241 billion.

[44] A. Colin Cameron and Pravin K. Trivedi, MICROECONOMETRICS USING STATA, Revised ed. (College Station, TX: StataCorp LP, 2010), pp. 300-301.

Exhibit B.2
Losses to the U.S. Economy Due to Delay in 5G Deployment Under Different Delay Scenarios

Year	5G Penetration Rate without Delay	5G Penetration Rate with Delay	GDP per Capita	Decline in GDP per Capita Because of Delay in 5G Deployment	U.S. Population Estimate	Decline in Total Annual Real GDP Because of Delay
6 Months Delay	**[A]**	**[B]**	**[C]**	**[D]=0.035* ([A]-[B])*[C]**	**[E]**	**[F]=[D]*[E]**
2018	0.00%	0.00%	$ 62,590	$ -	327,435,500	$ -
2019	0.13%	0.04%	$ 63,593	$ 2	329,685,382	$ 642,181,059
2020	0.50%	0.22%	$ 64,611	$ 6	331,950,723	$ 2,083,436,756
2021	2.82%	1.29%	$ 65,640	$ 35	334,231,630	$ 11,769,467,827
2022	8.04%	5.02%	$ 66,657	$ 71	336,528,209	$ 23,753,623,884
2023	19.85%	13.43%	$ 67,654	$ 152	338,840,569	$ 51,458,005,182
2024	33.92%	26.25%	$ 68,584	$ 184	341,168,817	$ 62,865,037,527
Discounted Present Value of Total Decline in GDP (in 2019 Dollars)						**$ 132,839,848,781.92**
12 Months Delay	**[A]**	**[B]**	**[C]**	**[D]=0.035* ([A]-[B])*[C]**	**[E]**	**[F]=[D]*[E]**
2018	0.00%	0.00%	$ 62,590	$ -	327,435,500	$ -
2019	0.13%	0.00%	$ 63,593	$ 3	329,685,382	$ 935,749,543
2020	0.50%	0.13%	$ 64,610	$ 8	331,950,723	$ 2,796,646,215
2021	2.82%	0.50%	$ 65,637	$ 53	334,231,630	$ 17,797,358,967
2022	8.04%	2.82%	$ 66,635	$ 122	336,528,209	$ 40,996,142,843
2023	19.85%	8.04%	$ 67,580	$ 279	338,840,569	$ 94,627,430,821
2024	33.92%	19.85%	$ 68,380	$ 337	341,168,817	$ 114,963,344,560
Discounted Present Value of Total Decline in GDP (in 2019 Dollars)						**$ 236,486,410,620.11**
18 Months Delay	**[A]**	**[B]**	**[C]**	**[D]=0.035* ([A]-[B])*[C]**	**[E]**	**[F]=[D]*[E]**
2018	0.00%	0.00%	$ 62,590	$ -	327,435,500	$ -
2019	0.13%	0.00%	$ 63,593	$ 3	329,685,382	$ 935,749,543
2020	0.50%	0.04%	$ 64,610	$ 10	331,950,723	$ 3,453,576,533
2021	2.82%	0.22%	$ 65,635	$ 60	334,231,630	$ 19,927,823,827
2022	8.04%	1.29%	$ 66,627	$ 158	336,528,209	$ 53,019,346,951
2023	19.85%	5.02%	$ 67,535	$ 351	338,840,569	$ 118,796,380,549
2024	33.92%	13.43%	$ 68,262	$ 490	341,168,817	$ 167,041,651,784
Discounted Present Value of Total Decline in GDP (in 2019 Dollars)						**$ 314,864,559,541.69**
24 Months Delay	**[A]**	**[B]**	**[C]**	**[D]=0.035* ([A]-[B])*[C]**	**[E]**	**[F]=[D]*[E]**
2018	0.00%	0.00%	$ 62,590	$ -	327,435,500	$ -
2019	0.13%	0.00%	$ 63,593	$ 3	329,685,382	$ 935,749,543
2020	0.50%	0.00%	$ 64,610	$ 11	331,950,723	$ 3,753,887,536
2021	2.82%	0.13%	$ 65,634	$ 62	334,231,630	$ 20,657,069,508
2022	8.04%	0.50%	$ 66,624	$ 176	336,528,209	$ 59,177,938,008
2023	19.85%	2.82%	$ 67,513	$ 402	338,840,569	$ 136,355,533,804
2024	33.92%	8.04%	$ 68,187	$ 618	341,168,817	$ 210,771,995,724
Discounted Present Value of Total Decline in GDP (in 2019 Dollars)						**$ 373,511,733,831.82**

Notes:
[1] I assume that without a delay in 5G deployment, 5G penetration rate between Q2 2019 and Q4 2024 would replicate 4G penetration rate between Q1 2009 and Q3 2014. I assume that if 5G deployment were delayed, 5G penetration rate would follow the same trajectory as in the scenario without delay, but its start would be delayed by the time equal to the duration of delay. For example, when 5G deployment is delayed by six months, 5G penetration rate is assumed to be zero in Q2 2019 and Q3 2019 and for t = Q4 2019-Q4 2024 it is assumed that the 5G penetration rate in Q_t equals the 5G penetration rate from the scenario without delay in Q_{t-2}. The annual penetration rate is calculated as the average of quarterly penetration rates.
[2] I assume that if 5G deployment is delayed, it will take 21 quarters, or 5.25 years, after the start of 5G deployment for the U.S. to reach the same penetration rate it would have if there were no delay in 5G deployment.
[3] The FCC intends to release mid-band spectrum to carriers in 2019-2020, but no date has been set. I assume that the mid-band spectrum will be released to carriers in Q3 2019, therefore, I assume that the delay associated with the spectrum gap is 6 months, or two quarters.
[4] I assume that a 1 percentage point decline in 5G penetration rate would result in a 0.035 percent decline in GDP per capita. This assumption is based on the regression estimates reported in Exhibit B.1.
[5] Real GDP per capita in [C] is assumed to grow at the rate of 1.6 percent per year. This growth rate is calculated as the compounded growth rate of annual real GDP per capita between 2012 and 2018, i.e., real GDP per capita growth rate = $(\text{real GDP per capita}_{2018}/\text{real GDP per capita}_{2012})^{(1/6)}-1$.
[6] U.S. population in [E] is assumed to grow at the rate of 0.69 percent per year. This growth rate is calculated as the compounded growth rate of U.S. population between 2012 and 2018, i.e., the population growth rate = $(\text{U.S. population}_{2018}/\text{U.S. population}_{2012})^{(1/6)}-1$
[7] The discounted present value of total decline in real GDP is calculated according to the following formula $\Sigma_{t=2019,\ldots2024}\text{Real GDP}_t/(1+0.035)^{(t-2019)}$, where 3.5 percent is the annual social discount rate from Mark A. Moore and Aidan R. Vining, "The Social Rate of Time Preference and the Social Discount Rate." *Mercatus Research Paper, December* (2018), p. 3, at https://www.mercatus.org/system/files/moore_and_vining_-_mercatus_research_-_a_social_rate_of_time_preference_approach_to_social_discount_rate_-_v1.pdf.

Sources:
[1] "Real gross domestic product per capita, Chained 2012 Dollars, Annual, Seasonally Adjusted Annual Rate," Federal Reserve Bank of St. Louis, accessed June 6, 2019, at https://fred.stlouisfed.org/series/A939RX0Q048SBEA.
[2] "Gross domestic product per capita, Dollars, Annual, Not Seasonally Adjusted," Federal Reserve Bank of St. Louis, accessed June 6, 2019, at https://fred.stlouisfed.org/series/A939RX0Q048SBEA#0.
[3] "Population, Thousands, Annual, Not Seasonally Adjusted," Federal Reserve Bank of St. Louis, accessed June 6, 2019, at https://fred.stlouisfed.org/series/POPTHM#0.
[4] Exhibits B.1 and B.3.
[5] GSMA Intelligence, "Country Dashboard," 2019, for the United States.
[6] "DataBank. World Development Indicators," The World Bank, Series "GDP per capita (constant 2010 US$)," "Trade (% of GDP)," "Net investment in nonfinancial assets (% of GDP)," "Labor force, total," at https://databank.worldbank.org/data/source/world-development-indicators.
[7] Mark A. Moore and Aidan R. Vining, "The Social Rate of Time Preference and the Social Discount Rate." *Mercatus Research Paper, December* (2018), at https://www.mercatus.org/system/files/moore_and_vining_-_mercatus_research_-_a_social_rate_of_time_preference_approach_to_social_discount_rate_-_v1.pdf, p. 3.
[8] Statement of Chairman Ajit Pai, Federal Communications Commission, Hearing on "Oversight of the Federal Communications Commission," Before the United States Senate Committee on Commerce, Science, and Transportation, June 12, 2019, available at https://docs.fcc.gov/public/attachments/DOC-357959A1.pdf.

i. Estimate of the Relationship Between Delay in 5G Deployment and Delay in 5G Adoption

19. Using GSMA 4G penetration rate data for Australia, Canada, China, Germany, Japan, South Korea, the United States, and the United Kingdom, I estimate the relationship between the duration of 4G deployment delay and the time it took a country to catch up with the penetration rate it would have had if its 4G deployment had not been delayed. I assume that this relationship will be the same for 5G.

20. To estimate that relationship, for each pair of countries for which 4G penetration started in different quarters, I identify the leader country and the follower country. I calculate the amount of delay as the number of quarters between the time when the leader country started deploying 4G and when the follower country started deploying 4G. I assume that without the delay, the follower country would have had the same trajectory of 4G penetration rate as the leader country. I calculate the number of quarters it took the follower country to catch up with the leader country in 4G penetration rate.[45] In 13 of the 27 country pairs, the

[45] I consider that a follower country catches up with a leader country if its 4G penetration rate stays consistently equal to or above the 4G penetration rate of the leader country.

4G penetration rate of the follower country never caught up with the 4G penetration of the leader country. If the follower country never caught up, I assign the catch-up time to be equal to 40 quarters, because 40 quarters is the average number of quarters between the quarter when a country started 4G deployment and the quarter when the same country started 5G deployment.[46]

21. I identified 27 country pairs in my data.[47] To estimate the relationship between the delay time and the catch-up time, I estimated the following regression:

$$Catch\ up\ Time_i = \beta_0 + \beta_1 * Delay\ Time_i + v_i, \quad (2)$$

where $Catch\ up\ Time_i$ is the time in quarters it took the follower country in country pair i to achieve the same 4G penetration rate as the leader country in that country-pair; $Delay\ Time_i$ is the number of quarters the follower country was behind the leader country in 4G deployment in country pair i; and v_i is the regression error term that captures idiosyncratic factors in country pair i that are not captured by the explanatory variables in the regression.

[46] There are only three countries in my sample that had deployed 5G mobile networks at the time of this report: South Korea, the United States, and the United Kingdom. The average number of quarters between the deployment of 4G and 5G equals 40.

[47] Australia and Canada reached non-zero 4G penetration rates in the same quarter. I did not include this country pair in my analysis.

Exhibit B.3
Estimated Impact of Delay in 5G Deployment on 5G Adoption

	Catch up Time
Delay Time	0.816**
	(0.333)
Constant	17.847***
	(5.483)
Observations	27
R^2	0.131

Note: ***significant at 99% level; ** significant at 95% level.

Source: GSMA Intelligence 2019 mobile subscriptions and statistics reports for Australia, Canada, China, Germany, Japan, South Korea, the U.K., and the U.S.

22. Using the regression results, I calculate the expected time it will take the United States to achieve the 5G penetration rate it would have achieved without delay. The predicted time to catch up equals 17.847 + 0.816 x delay time (in quarters), where the delay time takes values 2 quarters (delay associated with spectrum gap), and 4, 6, and 8 quarters (delay associated with spectrum gap plus the additional delay associated with the absence of Huawei from the U.S. market). I estimate that the predicted time of catch up for the assumed durations of delay of 2, 4, 6, and 8 quarters equals 4.87 years, 5.28 years, 5.69 year, and 6.09 years, respectively.

23. Based on these results, I assume for purposes of my estimate of the costs to the U.S. economy of delayed deployment of 5G networks due to excluding Huawei that the time to overcome the delay equals 5.25 years. This assumed delay is shorter than the estimated delay in each scenario in which an additional delay is caused by the absence of Huawei. This assumption is therefore conservative, because it shortens the period of 5G penetration rate delay in the scenarios where part of the delay is caused by Huawei's absence and increases the period of delay for the scenario where the entire delay is caused by the spectrum gap.

C. CALCULATION OF THE EFFECT ON EQUIPMENT VENDOR PRICES OF EXCLUDING HUAWEI FROM SALES OF RAN NETWORK EQUIPMENT IN THE UNITED STATES

24. Estimation of the extent to which prices for RAN equipment are higher in the United States due to the absence of Huawei requires several parameters: (1) revenue shares of the equipment vendors in the United States and an estimate of their shares in the but-for world in which Huawei is present and in the actual world in which Huawei is restricted; (2) diversion ratios between Huawei and its competitors; (3) gross margins of each company in the market for RAN equipment (including Huawei); and (4) ratios of Huawei's price to the prices of other firms in the market for RAN equipment when Huawei is present in the U.S. market. Below I discuss each of these parameters and how I calculated their values.

25. Because I do not have data on vendors' RAN equipment revenues shares in the United States, I assume that the vendors' RAN equipment revenue shares in the United States when Huawei is restricted from the market would be equal to the vendors' 2018 revenue shares in the market for all RAN equipment in North America. As I explained in Section VI of my report, vendors' revenue shares in North America primarily reflect vendors' revenue shares in the United States.

26. Huawei's revenue share in the United States if Huawei is allowed to participate in the U.S. market without any limitations is not observed, because Huawei has never been allowed to enter the U.S. market to the same extent as it has, for example, in Europe.[48] I consider three scenarios for what Huawei's revenue share would be if it were allowed to participate in the U.S. market: (1) Huawei's revenue share would equal its revenue share in Europe, (2) Huawei's revenue share would equal its average revenue share in all regions except North America, and (3) Huawei's revenue share would equal its average revenue share worldwide including the United States.[49]

27. I use revenue share data for 2018 because this is the most recent year for which data are available. To calculate the revenue shares of other vendors in the but-for world in which Huawei is present in the U.S. market, I apply the following formula:

---

[48] See Section VI of my report for background related to Huawei's current presence in the United States and the rest of the world.

[49] The revenue shares are calculated using the data provided by Dell'Oro Group.

$$rs_i = RS_i - D_{Hi}(rs_H - RS_H), \quad (3)$$

where rs_i is vendor i's revenue share in the United States in the but-for world in which Huawei is allowed to participate fully in the U.S. market; rs_H is the assumed revenue share of Huawei in the United States in the but-for world; RS_i is vendor i's revenue share in the United States in the actual world; RS_H is Huawei's revenue share in the actual world (as I explained in Section VI, Huawei has a very small revenue share in the United States serving primarily rural carriers); and D_{Hi} is the diversion ratio from Huawei to vendor i.

28. Diversion ratios quantify the extent to which products substitute for each other. The diversion ratio between two products is "the fraction of unit sales lost by the first product due to an increase in its price that would be diverted to the second product."[50] The higher is the diversion ratio between two vendors, the greater is the pricing discipline that the vendors' products impose on each other; and, conversely, the greater is the likelihood that one product's price will rise if the other is absent.[51]

29. I assume that the diversion ratio from product 1 to product 2 when firm 1 is absent from the market equals the revenue share of firm 2 divided by the sum of revenue shares of all firms in the market except firm 1.[52]

30. Gross margin is the difference between a firm's net sales revenue and its cost of goods sold, divided by net sales revenue.[53] I use each RAN vendors' gross margins provided by S&P Capital IQ Financial Communications as my estimate of its gross margin on RAN equipment.[54]

31. Finally, to calculate the ratio of Huawei's price to the price of another vendor (i.e., Ericsson, Nokia, Samsung, ZTE, and other) I use the global average sales prices of LTE-FDD products as provided by Dell'Oro Group. LTE-FDD is the most commonly deployed

---

[50] *2010 Horizontal Merger Guidelines*, Sec. 6.1.

[51] *2010 Horizontal Merger Guidelines*, Sec. 6.1.

[52] Carl Shapiro, "Mergers with Differentiated Products," *Antitrust*, Spring 1996, p. 25, at http://faculty.haas.berkeley.edu/shapiro/diversion.pdf.

[53] "Gross Margin Definition," Investopedia, at https://www.investopedia.com/terms/g/grossmargin.asp.

[54] S&P Capital IQ Financial Communications provides marketing and communications solutions and investor education for financial services firms. See "Company Overview of S&P Capital IQ Financial Communications," Bloomberg, at https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=22677616.

4G mobile wireless technology in the world.[55] Similar to 5G, it is not restricted to a single country or region (unlike some technologies in 2G and 3G), and therefore it is reasonable to assume that all of the equipment vendors produce material quantities of LTE-FDD equipment.[56]

32. If firms compete on prices and if demand is linear, the price increase of vendor *i* due to the restrictions on Huawei's participation in the market is analogous to a post-merger price increase of vendor *i*, and can be calculated according to the following formula:[57]

$$\frac{p_i^* - \overline{p_i}}{\overline{p_i}} = \frac{2D_{iH}M_H\frac{\overline{p_H}}{\overline{p_i}} + D_{Hi}(D_{iH} + D_{Hi})M_i}{4 - (D_{iH} + D_{Hi})^2} \quad (4)$$

where $\overline{p_H}$ and $\overline{p_i}$ are the prices of products sold by Huawei and vendor *i*, respectively (*i* indexes Ericsson, Nokia, Samsung, ZTE, and a hypothetical firm with the same market share as the remaining other firms) in the but-for world, and p_i^* is the price of firm *i* in the actual world; D_{Hi} measures the diversion ratio from Huawei's product to firm *i*'s product (that is, it is the share of sales lost by Huawei if it were to raise the price on its product that would be captured by firm *i*), and D_{iH} measures the diversion ratio from firm *i*'s product to Huawei's product (which is defined analogously to D_{Hi}).[58] Finally, M_H and M_i are gross profit margins of Huawei and firm *i*, respectively.

33. Exhibit C.1 shows the result of my analysis under the three assumptions of Huawei's revenue share in the United States if Huawei is allowed to sell RAN equipment in the

---

[55] See Section VII.C.

[56] I did not use prices of 5G RAN, because not all vendors had sales of 5G RAN equipment in Q4 2018 – Q1 2019, and Huawei's price dropped dramatically compared to prices of other vendors in Q1 2019. This may have occurred as a result of limitations placed on Huawei in several countries worldwide. See "M26A_5G_NR_Sub_6_GHz_Vendor Table_1Q19.xlsx" and "M27A_5G_NR_Millimeter_Wave_Vendor Table_1Q19.xlsx;" Katharina Buchholz, "Which Countries Have Banned Huawei?," Statista, May 21, 2019, at https://www.statista.com/chart/17528/countries-which-have-banned-huawei-products/.

[57] While this is a standard economic analysis, it incorporates several additional assumptions, including (1) that firms engage in Bertrand competition (i.e., firms are competing on prices), (2) that products offered by vendors in this market are close substitutes, and (3) that the marginal costs of firms in the market are constant. Carl Shapiro "Unilateral Effects Calculations," last updated: October 2010, at http://faculty.haas.berkeley.edu/shapiro/unilateral.pdf, pp. 2-5; Carl Shapiro, "Mergers with Differentiated Products," *Antitrust*, Spring 1996, pp. 24-27, at http://faculty.haas.berkeley.edu/shapiro/diversion.pdf.

[58] Carl Shapiro, "Unilateral Effects Calculations," last updated October 2010, at http://faculty.haas.berkeley.edu/shapiro/unilateral.pdf, p. 3.

United States. The exhibit indicates that in the absence of Huawei from the U.S. market for RAN equipment the prices of smaller vendors (Samsung, ZTE, and other vendors[59]) are higher by approximately 4.8-7.3 percent, Nokia's prices are higher by 12.5-15.8 percent, and Ericsson's prices are higher by 14.6-18.4 percent.

34. I also calculate the weighted average price effect, where each vendor's price increase is weighted according to its revenue share when Huawei is absent from the market. I estimate that, on average, Huawei's absence from the U.S. market for RAN equipment causes prices to be higher by 12.6-16.0 percent.

[59] These are vendors other than Huawei, Ericsson, Nokia, Samsung, and ZTE.

Exhibit C.1
Estimated Price Increase as a Result of Restrictions on Huawei's Participation in the U.S. Market for RAN Equipment

Vendor	Estimated Price Increase Resulting from Huawei's Absence From the U.S. Market (%)		
	Scenario 1: Huawei's Revenue Share in the U.S. in the Absence of Restrictions Equals Huawei's Revenue Share in Europe	Scenario 2: Huawei's Revenue Share in the U.S. in the Absence of Restrictions Equals Huawei's Revenue Share in All Regions Except North America	Scenario 3: Huawei's Revenue Share in the U.S. in the Absence of Restrictions Equals Huawei's Revenue Share Worldwide
ERICSSON	16.4%	18.4%	14.6%
NOKIA	14.0%	15.8%	12.5%
SAMSUNG	6.3%	7.3%	5.5%
ZTE	5.6%	6.4%	4.8%
OTHER	5.7%	6.5%	4.9%
Weighted Average	**14.2%**	**16.0%**	**12.6%**

Notes:

[1] I assume that gross margins for Huawei's and Samsung's network equipment, which are not reported separately from their handset and other business lines, are equal to Ericsson's gross margin for network equipment, which is a conservative assumption.

[2] Each vendor's price increase from the absence of Huawei from the U.S. market equals $[2*D_{iH}*M_H*(p_H/p_i)+D_{Hi}*(D_{Hi}+D_{iH})*M_i]/[4-(D_{Hi}+D_{iH})^2]$, where D_{Hi} is the diversion ratio from Huawei to vendor *i*; D_{iH} is the diversion ratio from vendor *i* to Huawei; M_H is Huawei's gross margin, M_i is vendor *i*'s gross margin, and p_H/p_i is the ratio of Huawei's price to vendor i's price when Huawei is present in the market; *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other. Other represents the combined market shares of all other vendors in the U.S.

[3] The diversion ratio from Huawei to vendor *i* is estimated as follows: $RS_H/(1-RS_i)$, where RS_i is the actual revenue share of vendor *i* in North America in 2018 and RS_H is the actual revenue share of Huawei in North America in 2018. The diversion ratio from vendor *i* to Huawei is estimated as $rs_i/(1-rs_H)$; where rs_i is the but-for revenue share of vendor *i* in North America in 2018 and rs_H is the but-for revenue share of Huawei in North America in 2018; and *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other.

[4] The ratio of Huawei's price to vendor *i*'s price is calculated as the ratio of the average sales price of Huawei's LTE FDD RAN products to the average sales price of vendor *i*'s LTE FDD RAN products in Q1 2019. The products used in this calculation include eNodeB macro, eNodeB micro, and eNodeB pico RAN equipment for LTE-FDD, and *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other.

[5] But-for revenue shares of vendors are calculated as follows: $rs_i = RS_i-(rs_H-RS_H)*D_{Hi}$, where RS_i is vendor i's actual revenue share in North America in 2018, RS_H is Huawei's actual revenue share in North America in 2018, rs_H is but-for Huawei's revenue share, D_{Hi} is the diversion ratio from Huawei to vendor *i*, and *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other.

[6] The weighted average price increase is calculated we follows:
$pi_{Ericsson}*rs_{Ericsson}+pi_{Nokia}*rs_{Nokia}+pi_{Samsung}*rs_{Samsung}+pi_{ZTE}*rs_{ZTE}+pi_{Other}*rs_{Other}$, where pi_i is the estimated price increase of vendor *i* and rs_i is the actual revenue share of vendor *i* in North America in 2018; *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other.

[7] The diversion ratio from Huawei to vendor *i* calculated using actual revenue shares is equivalent to diversion ratio from Huawei to vendor *i* calcualted using but-for revenue shares; and *i* indexes Ericsson, Nokia, Samsung, ZTE, and Other.

[8] Note that actual revenue shares of vendors in 2018 in North America and but-for revenue shares of vendors in North America are calculated using Dell'Oro data. Vendors' revenue shares are not displayed in the exhibit due to licensing restrictions on the Dell'Oro Group data.

Sources:

[1] "TOTAL GSM," "TOTAL CDMA," "TOTAL WCDMA," "TOTAL LTE," "TOTAL 5G NR," Dell'Oro Group, Q1 2019.

[2] "MOBILE RADIO ACCESS NETWORK – LTE – FDD," Dell'Oro Group, Q1 2019.

[3] "Huawei Investment Holding Co., Ltd., Financials," Available: S&P Capital IQ, McGraw Hill Financial.

[4] "Nokia Corporation," Available: S&P Capital IQ, McGraw Hill Financial.

[5] "Telefonaktiebolaget LM Ericsson," Available: S&P Capital IQ, McGraw Hill Financial.

[6] "Samsung Electronics Co., Ltd., KOSE A005930 Financials," Available: S&P Capital IQ, McGraw Hill Financial.

[7] "ZTE Corporation," Available: S&P Capital IQ, McGraw Hill Financial.

[8] Carl Shapiro, "Unilateral Effects Calculations," last updated October 2010, at http://faculty.haas.berkeley.edu/shapiro/unilateral.pdf, pp. 2-5.

D. STATE OF 5G DEPLOYMENTS IN THE UNITED STATES AND OTHER COUNTRIES

35. In this section I summarize the current status of 5G deployment at the time of this writing. Network deployments of new technology are highly dynamic and the status of network deployments may change rapidly.

i. United States

36. On October 1, 2018, Verizon launched a commercial millimeter wave ("mmW") 5G Fixed Wireless Access ("FWA") service called "Verizon 5G Home" using 28 GHz and 39 GHz bands in parts of Sacramento, Houston, Indianapolis, and Los Angeles. Verizon's network was launched using its own pre-standard 5G technology.[60]

37. On April 3, 2019, Verizon was first in the world to launch commercial 5G mobility (as opposed to FWA) networks. These were deployed in select areas in Chicago and Minneapolis. Verizon's 5G Ultra Wideband networks are accessible via two handsets: Motorola's Moto Z3 with 5G Moto Mod attachment (the attachment is required to access the 5G network), which is available only in the United States,[61] and Samsung's Galaxy S10 5G.[62] Verizon has announced that its 5G mobile networks will be available in 30 cities in 2019. Verizon's 5G network uses 28 GHz spectrum.[63]

38. On December 21, 2018, AT&T commercially launched 5G mobile networks using 39 GHz spectrum in selected areas of 12 cities: Atlanta, Charlotte (NC), Dallas, Houston, Indianapolis, Jacksonville (FL), Louisville (KY), Oklahoma City, New Orleans, Raleigh (NC), San Antonio, and Waco (TX). This service is available via the NETGEAR Nighthawk mobile hotspot device.[64] On June 17, 2019, AT&T started offering 5G services

---

[60] 2019 Global Race to 5G Analysys Mason Report, p. 9.

[61] Ed Adamczyk, "Verizon becomes first in the world to activate 5G network," UPI, April 3, 2019, at https://www.upi.com/Top_News/US/2019/04/03/Verizon-becomes-first-in-the-world-to-activate-5G-network/1901554310388/; Ahiza Garcia, "Verizon launches first 5G phone you can use on a 5G network in [sic] US," CNN Business, April 3, 2019, at https://www.cnn.com/2019/04/03/tech/verizon-5g-wireless-chicago-minneapolis/index.html.

[62] Todd Haselton, "The first 5G phone launches today for $1,300," CNBC, May 16, 2019, at https://www.cnbc.com/2019/05/16/samsung-galaxy-s10-5g-launches-on-verizon.html.

[63] Christian de Looper, "Verizon 5G rollout: Here is everything you need to know," Digital Trends, April 4, 2019, at https://www.digitaltrends.com/mobile/verizon-5g-rollout/.

[64] 2019 Global Race to 5G Analysys Mason Report, p. 9.

through its first 5G-capable phone—Samsung Galaxy S10 5G. This device was made available to AT&T's business customers and 5G developers only.[65] AT&T announced that in early 2020 it expects to offer a nationwide 5G footprint using sub-6 GHz spectrum.[66]

39. T-Mobile launched its 5G network on June 28, 2019.[67] T-Mobile's network is available in parts of six cities on the Samsung Galaxy S10 5G. Those cities are Atlanta, Cleveland, Dallas, Las Vegas, Los Angeles, and New York.[68] T-Mobile had announced earlier that it also would be deploying its 5G network on its 600 MHz spectrum.[69] The 5G network that T-Mobile launched on June 28th used mmW spectrum, like Verizon and AT&T. T-Mobile plans on using its low-band spectrum for further deployment.[70]

40. On May 30, 2019, Sprint launched its "true mobile" 5G in four cities across the United States: Atlanta, Dallas-Fort Worth, Houston, and Kansas City. Sprint has also announced plans to roll out 5G networks in parts of Chicago, Los Angeles, New York City, Phoenix, and Washington, D.C. in the coming weeks.[71] Sprint is using 2.5 GHz spectrum for its initial 5G rollout. Sprint announced that its network will be accessible through 5G-enabled LG V50 ThinQ and Samsung Galaxy S10 5G phones. Sprint is also offering 5G connectivity through its mobile hotspot—HTC 5G Hub.[72] In its 5G network, Sprint is

---

[65] "AT&T Business Launches Samsung Galaxy S10 5G," AT&T, June 12, 2019, at https://about.att.com/story/2019/samsung_galaxy_s10_5g.html.

[66] "First in the U.S. to Mobile 5G – What's Next? Defining AT&T's Network Path in 2019 and Beyond." AT&T, January 9, 2019, at https://about.att.com/story/2019/2019_and_beyond.html. It is not known from AT&T's statements whether AT&T is planning to deploy 5G in its low-band spectrum, or whether it expects to have obtained mid-band spectrum by that time.

[67] "Imagine a New T-Mobile: 5G for everyone, everywhere," T-Mobile, at https://www.t-mobile.com/5g?icid=WMM_TM_19NETWORK_UHIFVZ1BKZKJARS4J16163_HP.

[68] "T-Mobile to Carry the Samsung Galaxy S10 5G," T-Mobile Press Release, June 25, 2019, at https://www.t-mobile.com/news/samsung-galaxy-s10-5g.

[69] "T-Mobile Building Out 5G in 30 Cities This Year…and That's Just the Start," T-Mobile Press Release, February 26, 2018, at https://www.t-mobile.com/news/mwc-2018-5g.

[70] "T-Mobile to Carry the Samsung Galaxy S10 5G," T-Mobile Press Release, June 25, 2019, at https://www.t-mobile.com/news/samsung-galaxy-s10-5g.

[71] "Sprint Lights Up True Mobile 5G in Atlanta, Dallas-Fort Worth, Houston and Kansas City," Sprint Corporation Press Release, May 30, 2019, at https://newsroom.sprint.com/sprint-lights-up-true-mobile-5g-in-atlanta-dallas-fort-worth-houston-and-kansas-city.htm.

[72] "Sprint Lights Up True Mobile 5G in Atlanta, Dallas-Fort Worth, Houston and Kansas City," Sprint Corporation Press Release, May 30, 2019, at https://newsroom.sprint.com/sprint-lights-up-true-mobile-5g-in-atlanta-dallas-fort-worth-houston-and-kansas-city.htm; "Sprint U.S. Exclusive, HTC 5G Hub Delivers 5G Speed for Up to 20 Devices," Sprint, February 25, 2019, at https://newsroom.sprint.com/sprint-us-exclusive-htc-5g-hub-delivers-5g-speed-for-up-to-20-devices.htm.

deploying Massive MIMO provided by Ericsson, which it has deployed on its existing 4G cell sites and which are capable of simultaneously providing 4G LTE-Advanced and 5G service.[73]

ii. Australia

41. In December 2018, four mobile carriers in Australia won spectrum licenses in the 3.6 GHz band, which were allocated for 5G by the Australian Communication and Media Authority.[74] On May 22, 2019, Telstra launched its first 5G device—HTC 5G Hub—that works on Telstra's 5G mobile network in parts of 10 Australian cities.[75] It is expected that Telstra's 5G mobile network will reach at least 35 Australian cities by June 2020.[76] On May 28th, Telstra launched its first 5G-capable handset—Samsung Galaxy S10 5G.[77]

42. Optus has launched 5G FWA networks which are available to select customers in Brisbane, Adelaide, Perth, and some other areas. Optus plans to deploy over 1,000 5G sites by March 2020.[78]

43. Vodafone will be rolling out its 5G network in 2020.[79]

---

[73] "Sprint Lights Up True Mobile 5G in Atlanta, Dallas-Fort Worth, Houston and Kansas City," Sprint Corporation Press Release, May 30, 2019, at https://newsroom.sprint.com/sprint-lights-up-true-mobile-5g-in-atlanta-dallas-fort-worth-houston-and-kansas-city.htm.

[74] The 5G licenses allocated in the spectrum auction will start in March 2020. Juan Pedro Tomás, "Telecom Regulator ACMA said Australia raised over $615 million during the process," RCR Wireless, December 10, 2018, at https://www.rcrwireless.com/20181210/5g/four-australian-carriers-secure-5g-spectrum-band.

[75] "Telstra launches Australia's first 5G mobile device," Telstra Press Release, May 22, 2019, at https://www.telstra.com.au/aboutus/media/media-releases/Telstra_launches_Australias_first_5G_mobile_device; Jacqui Dent, "When can you get 5G in Australia," Whistle Out, June 17, 2019, at https://www.whistleout.com.au/MobilePhones/Guides/when-can-you-get-5G-in-Australia.

[76] "Australia's first 5G service goes live," Ericsson Press Release, May 22, 2019, at https://www.ericsson.com/en/news/2019/6/5g-live-in-australia-with-telstra.

[77] Kevin Teoh, "Australia's first 5G smartphone, the Samsung Galaxy S10 5G, is now in stores," Telstra Exchange, May 28, 2019, at https://exchange.telstra.com.au/australias-first-5g-smartphone-samsung-galaxy-s10-5g-now-in-stores/.

[78] Tim Fisher, "When Is 5G Coming to Australia? (Updated for 2019)," July 1, 2019, Lifewire, at https://www.lifewire.com/5g-australia-4583137.

[79] Jacqui Dent, "When can you get 5G in Australia," Whistle Out, June 17, 2019, at https://www.whistleout.com.au/MobilePhones/Guides/when-can-you-get-5G-in-Australia.

iii. China

44. China has yet to launch a commercial 5G network. In December 2018, the Chinese Ministry of Industry and Information Technology ("MIIT") distributed spectrum licenses in the 3.5 – 3.6 GHz, 3.4 – 3.5 GHz, 2.515 – 2.675 GHz, and 4.8 – 4.9 GHz bands to the three major Chinese carriers for 5G trials.[80] On June 6, 2019, MITT awarded commercial licenses to the same companies in the same bands.[81] China Mobile has announced plans to roll out 5G networks in more than 50 cities by the end of 2019, ahead of the earlier Chinese timeline, which planned for commercial 5G rollout in 2020.[82]

iv. Japan

45. No Japanese telecommunications company has launched a 5G network at the time of this report. In April 2019, Japanese regulators allocated mid-band and high-band 5G spectrum (3.6 GHz – 4.6 GHz and 27.0 GHz –29.5 GHz) to telecommunications companies, and Japanese carriers plan to begin commercial 5G services in 2020.[83] The conditions of Japan's spectrum allocation require these carriers to deploy in every prefecture within two years.[84] The earliest estimates, from KDDI and Softbank, project launches of 5G networks

---

[80] "China issues 5G trial spectrum permits," *Telegeography*, December 10, 2018, at https://www.telegeography.com/products/commsupdate/articles/2018/12/10/china-issues-5g-trial-spectrum-permits/index.html. "MIIT awards 5G licences to three MNOs plus cable operator," *Telegeography*, June 6, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/06/06/miit-awards-5g-licences-to-three-mnos-plus-cable-operator/index.html.

[81] "MIIT awards 5G licences to three MNOs plus cable operator," *Telegeography*, June 6, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/06/06/miit-awards-5g-licences-to-three-mnos-plus-cable-operator/index.html.

[82] Juan Pedro Tomás, "China Mobile to launch 5G in 50 cities across China by end-2019," *RCR Wireless*, June 26, 2019, at https://www.rcrwireless.com/20190626/5g/china-mobile-launch-5g-50-cities-china-end-2019.

[83] "MIC approves allocation of 5G spectrum to Japanese operators, with conditions," *Telegeography*, April 11, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/04/11/mic-approves-allocation-of-5g-spectrum-to-japanese-operators-with-conditions/index.html.

[84] "MIC approves allocation of 5G spectrum to Japanese operators, with conditions," *Telegeography*, April 11, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/04/11/mic-approves-allocation-of-5g-spectrum-to-japanese-operators-with-conditions/index.html.

in March 2020.[85] While Japan's timeline is later than those of the United States and South Korea, Japan has now allocated both mid- and high-band spectrum for 5G use.[86]

v. South Korea

46. On December 1, 2018, South Korean carriers SK Telecom, KT, and LG Uplus launched 5G Fixed Wireless Access ("FWA") services. These services were launched simultaneously by the three carriers in selected locations to select individuals.[87] On April 3, 2019, SK Telecom, KT, and LG Uplus opened commercial wireless 5G network to the general public. The networks became accessible to other subscribers on April 5, 2019, when Samsung's 5G smartphone Galaxy S10 5G was launched in South Korea.[88] As of June 12, 2019, the three South Korean carriers announced that they had collectively enrolled 1 million 5G subscribers.[89] Each of the South Korean carriers holds large spectrum blocks in both mid- and high-band spectrum.[90]

vi. Switzerland

47. On April 4, 2019 Swiss telecommunications operator Sunrise launched FWA 5G in more than 150 cities/villages.[91] Sunrise's 5G network will be available via its Sunrise Internet

---

[85] "MIC approves allocation of 5G spectrum to Japanese operators, with conditions," *Telegeography*, April 11, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/04/11/mic-approves-allocation-of-5g-spectrum-to-japanese-operators-with-conditions/.

[86] "MIC approves allocation of 5G spectrum to Japanese operators, with conditions," *Telegeography*, April 11, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/04/11/mic-approves-allocation-of-5g-spectrum-to-japanese-operators-with-conditions/.

[87] *2019 Global Race to 5G Analysys Mason Report*, pp. 9-10; Tim Fischer, "When Is 5G Coming to South Korea? (Updated for 2019)," Lifewire, April 5, 2019, at https://www.lifewire.com/5g-south-korea-4583813.

[88] Tim Fischer, "When Is 5G Coming to South Korea? (Updated for 2019)," Lifewire, April 5, 2019, at https://www.lifewire.com/5g-south-korea-4583813; Nidhi Singh, "Here's the World's First Country to Launch 5G Services," Entrepreneur Asia Pacific, April 5 2019, at https://www.entrepreneur.com/article/331801.

[89] Jeremy Horowitz, "South Korea hits 1 million 5G subscribers in 69 days, beating 4G record," Venture Beat, June 12, 2019, at https://venturebeat.com/2019/06/12/south-korea-hits-1-million-5g-subscribers-in-69-days-beating-4g-record/.

[90] *2019 Global Race to 5G Analysys Mason Report*, pp. 9, 67.

[91] "'5G for People' has started: First Sunrise customers are using 5G," Sunrise Press Release, April 4, 2019, at https://e3.marco.ch/publish/sunrise/821_3894/20190404_MM_First_5G_Pioneer_EN.pdf.

Box 5G device.[92] Sunrise also launched 5G networks on April 17, 2019 in 54 cities in Switzerland. Sunrise offers 5G smartphones through the Huawei Mate 20 X.[93]

48. Swisscom is offering connection to its 5G network through three mobile phones: the Oppo Reno 5G, LG V50 ThinQ, and Samsung Galaxy S10 5G.[94] Swisscom's network is the first large-scale commercial 5G network in Europe to support commercially available smartphones, and it was launched in partnership with Ericsson.[95] Both Sunrise and Swisscom launched their networks on spectrum from a February 2019 auction, in which both Sunrise and Swisscom purchased spectrum in the 700 MHz, 1400 MHz, and 3500 MHz (3.5 GHz) ranges.[96]

vii. United Kingdom

49. In the United Kingdom, carrier EE launched mobile commercial 5G networks in parts of six major cities at the end of May 2019.[97] EE offers 5G service through the OnePlus 7 Pro 5G, Oppo Reno 5G, LG V50 ThinQ, and Samsung Galaxy S10 5G phones.[98] EE's 5G networks are also available via either mobile broadband device or home broadband router.[99] Vodafone launched 5G commercial networks in seven British cities on July 3, 2019. Vodafone's 5G networks are accessible via two mobile phones, the Xiaomi Mi Mix

---

[92] "Sunrise unveils 5G plans," *TeleGeography*, February 21, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/02/21/sunrise-unveils-5g-plans/. Sunrise Internet Box 5G device is not yet available for purchase at Sunrise's website. See "Hotspots," Sunrise, at https://www.sunrise.ch/en/residential/geraete/hotspots.html#/.

[93] "Sunrise and Huawei Jointly Announce First 5G Smartphone in Switzerland," Huawei Press Release, May 8, 2019, at https://www.huawei.com/en/press-events/news/2019/5/sunrise-huawei-jointly-announce-first-5g-smartphone; Juan Pedro Tomás, "Ericsson, Swisscom launch commercial 5G network in Switzerland," RCWireless News, April 17, 2019, at https://www.rcrwireless.com/20190417/5g/ericsson-swisscom-5g.

[94] Jeremy Horwitz, "Swisscom debuts Europe's first commercial 5G service with May phone launch," April 10, 2019, at https://venturebeat.com/2019/04/10/swisscom-debuts-europes-first-commercial-5g-service-with-may-phone-launch/.

[95] "Ericsson and Swisscom in European commercial 5G first," Ericsson Press Release, April 17, 2019, at https://www.ericsson.com/en/press-releases/2019/4/ericsson-and-swisscom-in-european-commercial-5g-first.

[96] "Switzerland completes 5G auction," *Telegeography*, February 8, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/02/08/switzerland-completes-5g-auction/.

[97] "EE launches 5G in six cities," *Telegeography*, May 31, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/05/31/ee-launches-5g-in-six-cities/index.html.

[98] "Discover 5G," *EE*, at https://ee.co.uk/why-ee/5g-on-ee.

[99] "EE launches 5G in six cities," *Telegeography*, May 31, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/05/31/ee-launches-5g-in-six-cities/index.html.

3 and the Samsung S10 5G, and a 5G router.[100] Carrier Three is set to launch in London in August.[101]

50. Ofcom, the British agency that regulates spectrum, auctioned 2.3 GHz and 3.4 GHz spectrum in 2018 and has plans to award the 700 MHz low-band and 3.6-3.8 GHz mid-bands in December 2019.[102]

viii. United Arab Emirates

51. In November 2018, the Telecommunications Regulatory Authority ("TRA") of the United Arab Emirates ("UAE") issued 5G spectrum in the mid band (3.3-3.8 GHz) to Etisalat and Du, the country's two largest telecommunications companies.[103] Both Etisalat and Du are selling ZTE's Axon 10 Pro smartphone, which is 5G capable, but neither Etisalat nor Du plan to launch commercial 5G services until 2020.[104] Du plans to launch its service in late 2019 and Etisalat plans to launch 5G in 2020.[105]

---

[100] Paul Sandle, "Vodafone launches 5G in Britain with unlimited data plans," *Reuters*, July 3, 2019, at https://uk.reuters.com/article/us-vodafone-5g-britain/vodafone-launches-5g-in-britain-with-unlimited-data-plans-idUKKCN1TY2EC.

[101] "UK mobile operator Three to launch 5G broadband in August," *Reuters*, June 9, 2019, at https://www.reuters.com/article/us-three-5g/uk-mobile-operator-three-to-launch-5g-broadband-in-august-idUSKCN1TA0V4.

[102] "Ofcom's Annual Plan: Our programme of work for 2019/20," Ofcom, March 25, 2019, ¶¶ 2.8, 3.8.

[103] "TRA confirms UAE 5G spectrum allocations," *Telegeography*, November 19, 2018, at https://www.telegeography.com/products/commsupdate/articles/2018/11/19/tra-confirms-uae-5g-spectrum-allocations/index.html.

[104] "Du hot on the heels of Etisalat with 5G launch," *Telegeography*, June 3, 2019, at https://www.telegeography.com/products/commsupdate/articles/2019/06/03/du-hot-on-the-heels-of-etisalat-with-5g-launch/index.html.

[105] "Etisalat Completes the Fastest 5G," Etisalat Press Release, https://www.etisalat.ae/en/about-us/media_center/press_releases/etisalat_g.jsp. "du's 5G Experience Goes Live This Ramadan," Du Press Release, May 21, 2019, at https://www.du.ae/about/media-centre/newsdetail/du-5g-experience-goes-live-this-ramadan.

Exhibit 16

10/31/2019 Huawei Ex Parte
(rebutting the Finite State Report)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket. In particular, Huawei responds to the *Draft Report and Order*'s citation to a 2019 report by Finite State (the "Finite State Report") which purports to assess the security of Huawei's products and services.[1]

Huawei has publicly responded to the Finite State Report, highlighting significant flaws in the methodology used and factual errors that undercut the Report's conclusions. Attached as **Exhibit 1** is a statement released by Huawei regarding the Finite State Report, and a technical analysis of the Finite State Report performed by Huawei's Product Security Incident Response Team ("PSIRT") is attached as **Exhibit 2**.

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Draft Report and Order, Order, and Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC-CIRC1911-01, para. 51 (circulated Oct. 29, 2019) ("*Draft Report and Order*") (citing Finite State, Finite State Supply Chain Assessment at 3 (2019), https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf) ("*Finite State Report*").

In summary, the Finite State Report is replete with basic errors. Although it asserts otherwise, the Finite State Report evaluated old versions of Huawei's products and identified issues that had been fixed in updated versions of these products. The Finite State Report bases some of its conclusions about potential backdoors on the assumption that Huawei uses standard Linux-based authentication,[2] but it does not. More generally, Finite State failed to follow general practices of responsible security testing companies, which typically involves dialogue between the security company and vendor about alleged vulnerabilities to help ensure a complete and accurate picture of security vulnerabilities. The Report also contains no explanation of how Finite State selected the vendors it used for purposes of comparison in its study, why it ignored the vendor who holds the largest market share of the global enterprise network, or why it tested almost all of the hundreds of Huawei enterprise network products, but only one product each of Juniper and Arista without disclosing the versions assessed. The Finite State Report also includes a background section that includes unsupported and erroneous assertions. For example, it cites erroneous reporting suggesting that Vodafone found an alleged "backdoor" in Huawei's equipment in Italy.[3] But Vodafone itself has explained that the alleged backdoor was no backdoor at all and the issue was resolved in 2011 and 2012.[4]

---

[2] *See Finite State Report*, at 27.

[3] *See Finite State Report*, at 5 (asserting, incorrectly, that Vodafone had found vulnerabilities associated with Huawei equipment).

[4] *See* "Vodafone denies Huawei Italy security risk," BBC News, (Apr. 30, 2019), https://www.bbc.com/news/business-48103430 (noting "In a statement, Vodafone said: 'The issues in Italy identified in the Bloomberg story were all resolved and date back to 2011 and 2012[]'" and that Vodafone has "'no evidence of any unauthorised [sic] access. This was nothing more than a failure to remove a diagnostic function after development.'").

The *Draft Report and Order* is bereft of *any* assessment of the methodology or the accuracy of the assertions made in the Finite State Report and simply accepts the Report's conclusions at face value. That is untenable in light of the many easily discoverable errors in the Finite State Report. The Commission's reliance on the Finite State Report to support its conclusion that Huawei poses national security risk to communications networks in the United States would be irrational, arbitrary, and capricious. As Huawei has extensively advocated in this proceeding and elsewhere, a risk-based security approach, including the use of independent, third-party testing of products from all equipment vendors using internationally recognized standards, will do far more to protect communications infrastructure in the United States and elsewhere from cybersecurity vulnerabilities than banning the use of equipment by specific vendors.

Respectfully submitted,

/s/ Andrew D. Lipman

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

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

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

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

October 31, 2019

EXHIBIT LIST

Exhibit 1: "Finite State Report Fails to Tell the Whole Story"

Exhibit 2: Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment

Exhibit 16-A

"Finite State Report Fails to Tell the Whole Story"

Finite State report fails to tell the whole story

Huawei is serious about cyber security and welcomes any objective input that makes our technology more secure. This includes analyses that publicly disclose any weaknesses our products may have.

On June 25, a US cyber security firm called Finite State released a report saying Huawei products were more vulnerable than equipment made by some of our competitors. We have a Product Security Incident Response Team (PSIRT) that discloses vulnerabilities in our products when we find them. PSIRT and our engineers published an in-depth response to the technical points of Finite State's analysis.

The Finite State report is a preliminary assessment, very much like the ones Huawei (and every vendor of network equipment) conducts to test the integrity of our products. As a preliminary assessment, it does not tell the whole story.

Our initial review suggests that the data cited in their report, and the testing methods they used, would not identify significant vulnerabilities in Huawei's gear.

First, many of the products critiqued are for enterprise markets, with some data center switches for the carrier market. None of the Huawei products tested by Finite State will be deployed for 5G RAN or Core in telecommunications networks. (Products made by Cisco, the largest provider of gear for the enterprise market, were not tested.)

Second, Finite State used something called a binary image analysis tool. The tool is suitable for certain narrow security applications but cannot provide a complete and accurate picture of security vulnerabilities in the products tested.

Third, Finite State specializes in security for the Internet of Things (IoT) and may not fully understand how telecommunications equipment is deployed. For example, an important fact not referenced in the report is that after installation, default settings are zeroed out, providing network operators with secure control over their equipment. Equipment vendors also work closely with operators to address potential vulnerabilities, such as those that might be disclosed using a tool like the one Finite State used for this study.

Fourth, Finite State tested older versions of Huawei software, which might not have contained important security patches issued later. It is not clear why Finite State chose older versions when newer ones were available. We don't know how Finite State obtained the software they used, and we don't know which distribution channel they used as a source.

Finally, and significantly, Finite State did not give Huawei a chance to review its analysis before publication. Normally, firms that conduct independent analysis strive to present neutral, unbiased research; accordingly, they check any findings with the affected vendors before going public. Finite State's failure to do that raises questions about their motivation in releasing the report. More importantly, the report lacks important insights that could have been provided to make it more complete, and more accurate.

The inclusion of extraneous, negative information about Huawei also suggests that objectivity was not a major consideration. For example, several pages outline "Key security concerns" about Huawei, setting a negative tone at the outset and suggesting a presumption that Huawei products are flawed.

Finite State also cited a Bloomberg story which incorrectly reported that Vodafone had found "backdoors" in Huawei's network gear in Italy. Vodafone quickly corrected the report, explaining that what Bloomberg had mistakenly called a backdoor was, in fact, part of a routine diagnostic function commonly used in the telecommunications industry. Yet, although Vodafone published the official statement in April, Finite State's June report still cited the erroneous Bloomberg story and did not mention the correction.

Huawei is committed to securing critical network infrastructure. We work with independent researchers and testing firms worldwide to find, and fix, vulnerabilities that might compromise security. Because we are headquarted in China, we are probably the most frequently, most thoroughly tested technology provider in the world. Even so, no one has ever found any evidence of cyber security wrongdoing in our equipment. Because of the important insights gained from expert, independent reviews of our technology, we will spend US$2 billion in the coming years to revamp our software engineering processes and improve our software quality and security.

Again, we have no problem letting people pick apart our software; in fact, we have facilities dedicated to doing just that. But the testing methodology employed by Finite State is not, by itself, sufficient to provide what the global community needs: an objective, transparent method of testing the products sold by technology providers based on uniform global standards.

That said, we would welcome the opportunity to speak with Finite State about their findings, in hopes of gaining insights that can help us improve our practices and further inform our software engineering revamp.

Finite State's report implicitly supports Huawei's longstanding call for independent, third-party testing of products from all equipment vendors, using internationally recognized standards. Such an approach would help move important conversations about cyber security away from the realm of politics, toward the domain of science, engineering, and facts. And that would help make cyberspace a safer place.

July 9, 2019

Huawei Technologies Co., Ltd.

Exhibit 16-B

Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Read our privacy policy (update in May 2018) >

Huawei PSIRT: Technical Analysis Report Regarding Finite State Supply Chain Assessment

Last Release Date: Jul 03, 2019

At Huawei, we welcome collaboration with cyber security researchers and independent testing of our products and solutions. We have a long-established Product Security Incident Response Team (PSIRT) that manages the collection, investigation, internal coordination and responsible disclosure of security vulnerability information related to Huawei products. Once a vulnerability has been confirmed, PSIRT promptly conveys the information to the teams responsible for the affected products, and then actively tracks the progress to resolution.

Huawei has built and implemented a multi-tiered end-to-end cyber security evaluation process to ensure that our products are reviewed for potential security issues from product concept, design, development, and right throughout to deployment and maintenance in our customers' networks around the world.

On June 26, 2019, U.S.-based Finite State publicly disclosed the *Supply Chain Assessment* report about Huawei on its official website. In this report, Finite State describes its use of a static analysis tool for firmware images (binary software packages) to analyze more than 500 Huawei enterprise network products and the comparison analysis between Huawei CE12800, Juniper EX4650, and Arista 7280R, with conclusions that Huawei products have poorer security and potential backdoors.

We were surprised and disappointed by the unconventional approach of Finite State. We cannot determine whether Finite State obtained the software from legitimate channels or guarantee its integrity, nor has Huawei ever received any communication requests from Finite State. They made no contact with Huawei to assist them in their understanding and refused to provide a copy of their analysis before it was published. Sadly, this means what has been published lacks the insight, integrity and accuracy we would normally expect from a professional, serious and capable organization.

Due to the approach Finite State has taken and the weakness of their tools and methodology, the results are at best suspect and at worst just inaccurate. This could have been avoided by collaborating rather than taking a political stance on security.

We are unsure of the objectives of the CEO Matt Wyckhouse and Finite State overall and why they did not select the market leader Cisco for comparison, or indeed why they evaluated old versions of Huawei products and identified issues that had been fixed in new versions.

Whilst Finite State has had many months to undertake their flawed analysis, over the last few days Huawei PSIRT has investigated the issues mentioned in the report immediately after the report was published. We believe that the approach used by Finite State has serious operational and technical defects, the tests lack neutrality, and the report contains material inaccuracies.

1 Finite State's Test Process and Report Development Approach Are Contrary to General Practices of Responsible Security Testing Companies

Responsible disclosure of security issues or vulnerabilities is widely recognized and practiced by the industry. Typically, security research organizations or researchers deliver identified issues and potential vulnerabilities to vendors, and vendors then confirm whether they are defects or vulnerabilities and carry out coordinated handling. Finite State simply used a tool to scan raw binaries and then conducted simple partial reverse analysis of some potential issues to reach their conclusions. Finite State has not used vulnerability exploitation in real-world products to verify the analysis, nor has the analysis been confirmed by Huawei product R&D. Binary vulnerability scanning tools are generally used for auxiliary analysis because their error rate can reach up to over 90%. Thus, Finite State's conclusions are drawn in a hasty manner and are inaccurate. Although Finite State mentions the limitations of the tool it has developed and used, for example, the tool does not support analysis in context, and vulnerabilities are based on file names and version information, Finite State has overestimated the sophistication and accuracy of its tool. As we demonstrate in Appendix, independent analysts do not rank Finite State tools as market leaders in any dimension.

Finite State made a hasty and unprofessional decision to deliver the assessment report to the media and government authorities, without providing it to Huawei beforehand, nor have the issues been confirmed by Huawei. This practice is contrary to best practice or even basic common sense in terms of responsible security organizations in the industry. A fair security technology organization shall remain neutral and express opinions from the perspective of technical security.

Finite State's assessment report repeatedly mentions potential backdoors in Huawei products in an emotional and overstated way. Any security company that claimed it has discovered many backdoors and unfixed serious vulnerabilities by tool-based scanning and without verifying the products or even having any context or knowledge of the products, their architecture and environment, cannot be taken seriously.

2 Assessment Report Gives No Explanation About the Selection of Vendors, Products and Versions for Comparison, and Selective Tests Have Been Conducted

The assessment report does not explain why products of Huawei, Juniper, and Arista were used as test samples but Cisco, another company who holds the largest market share of the global enterprise network. Why weren't Cisco products evaluated? Finite State tested almost all of the hundreds of Huawei enterprise network products, but only one product of Juniper and Arista without disclosing their versions. According to the report, it states that the latest versions of Huawei products are used, however, all versions mentioned in the report are actually old versions. For example, AR1200 V200R007C00SPCc00 released in 2017 was used. However, the updated versions released in 2018 and 2019, such as V200R009 and V200R010, are available on Huawei's technical support website. Moreover, AR3600 V200R007C00SPCb00 released in 2016 was used, but the updated versions released in 2018 and 2019, such as V200R008 and V200R009, are also available on Huawei's technical support website.

We believe selective tests have been conducted, with intentionally selected versions and comparison objects to achieve the "expected" results for Finite State or those that funded this "research".

3 Finite State's Conclusions Are False Through Our Investigation and Analysis

Regarding Finite State's conclusions, Huawei products have backdoors and many vulnerabilities or even serious vulnerabilities left unfixed, Huawei PSIRT and R&D have undertaken a detailed analysis and reached the following conclusions after verification.

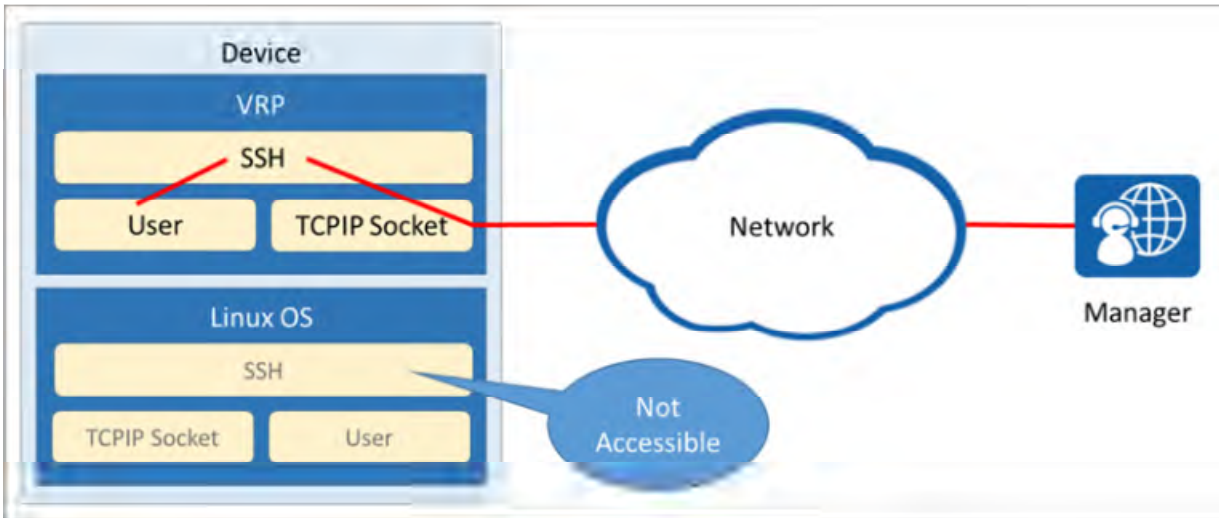
3.1 Analysis of Suspected Backdoors

Many suspected backdoor conclusions drawn by Finite State are based on the prerequisite that Huawei is using standard Linux-based authentication. However, this prerequisite is incorrect and thereby the stated conclusions are wrong.

3.1.1 Analysis of Undocumented and Hard-coded Credentials

The report shows that *huawei*, *python*, and *root* accounts are potential privilege escalation backdoors. In fact, the three accounts identified cannot be used for unauthorized privilege escalation. The analysis is as follows:

Huawei AR products use only basic functions of Linux, such as task scheduling. Other functions, namely, user management, remote access control, and TCP/IP protocol stack, are taken over by Huawei Versatile Routing Platform (VRP). This design can better meet application requirements of products. Many telecommunications companies in the industry also use the similar design pattern, as shown in the following figure.



VRP taking over remote user access

The *root* account is used to start the VRP process. It is used internally and invisible externally. The *python* and *huawei* accounts are used by VRP users with the highest privileges to create VMs and install third-party applications. These accounts are invisible externally. The three accounts are protected from being exploited for remote device access and do not compromise system security.

It is true that the sudo configuration and sbin/insmod commands mentioned in the report may be exploited for privilege escalation. Huawei PSIRT has confirmed that this is a known and fixed vulnerability. The device administrator shall be assigned the least privilege to reduce risks. Huawei has eliminated the risk in V300R003C00SPC500

(released in August 2018) by using the program code to implement related management functions.

In addition, the *huawei*, *python*, and *root* accounts are documented in *Command Reference* (2018)

3.1.2 Analysis of Default Hard-coded Cryptographic Keys

As described in the report, the authorized_keys and similar files are engineering tools used during the development process. The E9000 and CE12800 R&D engineers use SSH of the Linux OS to facilitate debugging, and leave the key files in the firmware.

As illustrated in section 3.1.1"Analysis of Undocumented and Hard-coded Credentials", Huawei datacom products use the basic functions of Linux. Remote access control and TCP/IP protocol stack are taken over by the VRP. In official versions, the debugging function is disabled, and external users cannot access SSH of the Linux OS. Therefore, these key files do not cause any potential unauthorized access. These key files will be deleted in the version to be released in September 2019.

The report shows the presence of an authorized_keys file for the superuser account on the firmware image of SmartAX MA5800, but the SSH code has been deleted from the released versions, and therefore no security risks exist.

3.2 Analysis of Known Vulnerabilities Not Fixed

The report describes the use of outdated components and we agree with this analysis and have already announced substantial upgrades to enhance our products in this regard... However, the presence of outdated components does not necessarily mean the presence of security issues.

The known vulnerability analysis method SCA mentioned in the report is used to assess known vulnerabilities by open-source software name and version number. This method is defective for embedded devices because of the following causes:

(1) Code related to open-source component vulnerabilities is not compiled into the firmware.

(2) For some open-source software, after a vulnerability is detected, the source code patch will be preferentially released to fix the vulnerability. Then a formal fix version is planned. This process may take a long time depending on the open source community approach. To fix the vulnerability as soon as possible, telecom vendors usually incorporate the fixed source code. However, the version number of the open-source software used in the product firmware is still the old version number.

(3) The method of fixing vulnerabilities using binaries is similar to (2). The version number of the open-source software remains unchanged.

(4) The vulnerable code in the open-source component is included in the firmware, but the corresponding functional module is not used.

After analyzing the 10 well-known vulnerabilities reported in AR3600 V200R007C00SPCb00, we find that 6 vulnerabilities cause no impact, 2 are fixed, and 2 are of low risks. The details are as follows:

Vulnerability Name	Component	CVE ID	Analysis Result
DROWN	OpenSSL	CVE-2016-0800	This vulnerability affects only SSL V2. The earliest version supported by products is SSL V3.
FREAK	OpenSSL	CVE-2015-0204	The vulnerability is fixed by incorporating the fixed code, but the OpenSSL version remains unchanged.
POODLE	OpenSSL	CVE-2014-3566	The vulnerability is fixed by incorporating the fixed code, but the OpenSSL version remains unchanged.
Heartbleed	OpenSSL	CVE-2014-0160	The vulnerable openssl1.0.1e is used on cards, but the OpenSSL function on the cards is not used.
Quadrouter	Linux Kernel	CVE-2016-2059	The kernel is tailored, and the vulnerable code is not included in the product package.
Quadrouter	Linux Kernel	CVE-2016-5340	The kernel is tailored, and the vulnerable code is not included in the product package.
Linux Kernel	Linux Kernel	CVE-2016-5696	This vulnerability is present in the TCP/IP protocol stack of the Linux kernel. It is involved only when the AR3600 needs to load the system software package in boot mode (only in the case of serial port access). In other cases, this protocol stack is not used. Therefore, the security risk is low.
Linux Kernel	Linux Kernel	CVE-2016-0728	The kernel is tailored, and the vulnerable code is not included in the product package.
NA	Linux Kernel	CVE-2016-10229	This vulnerability is present in the TCP/IP protocol stack of the Linux kernel. It is in-

Vulnerability Name	Component	CVE ID	Analysis Result
			volved only when the AR3600 needs to load the system software package in boot mode (only in the case of serial port access). In other cases, this protocol stack is not used. Therefore, the security risk is low.
NA	OpenSSL	CVE-2016-7055	This vulnerability is present in OpenSSL 1.0.2, 1.1.0c, and earlier versions. Products use OpenSSL 1.0.1 and therefore are not affected.

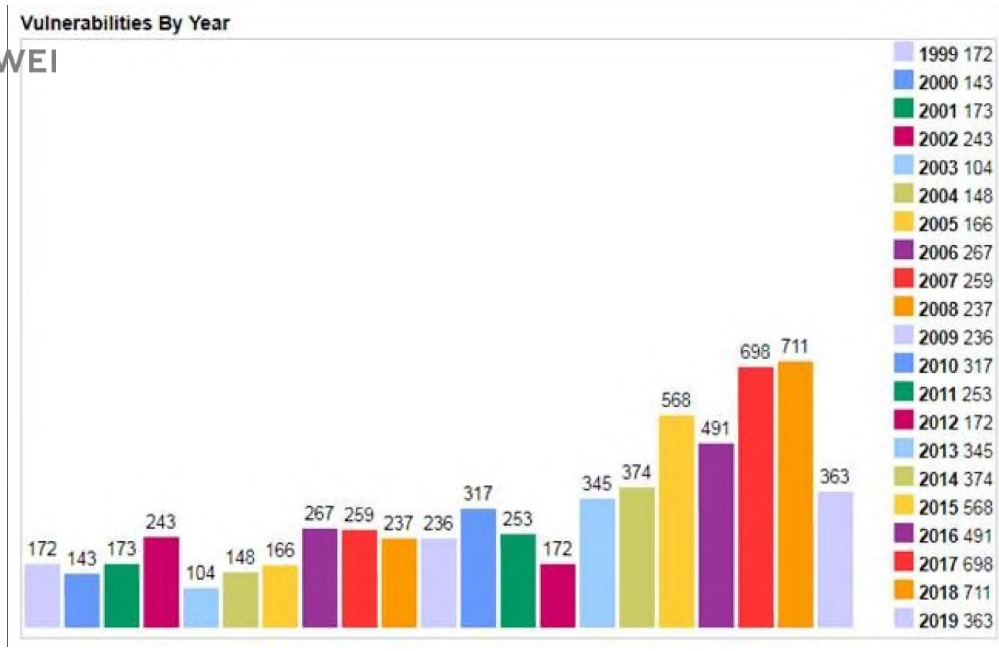
3.3 Analysis of Conclusion that Huawei Situation Is Getting Worse Drawn on An Increased Number of Publicly Known CVE Vulnerabilities

Finite State concluded on page 23 of the report that the situation of Huawei is getting worse based on an increased number of CVEs, which is unscientific.

It is a basic requirement of ISO/IEC 29147:2018 Vulnerability Disclosure to disclose a vulnerability to customers and notify them of risks and mitigations after fixing the vulnerability. Huawei PSIRT is a dedicated global vulnerability response team which established Huawei's vulnerability response process based on related standards. In 2012, Huawei PSIRT established a public channel (www.huawei.com/psirt) for vulnerability disclosure.

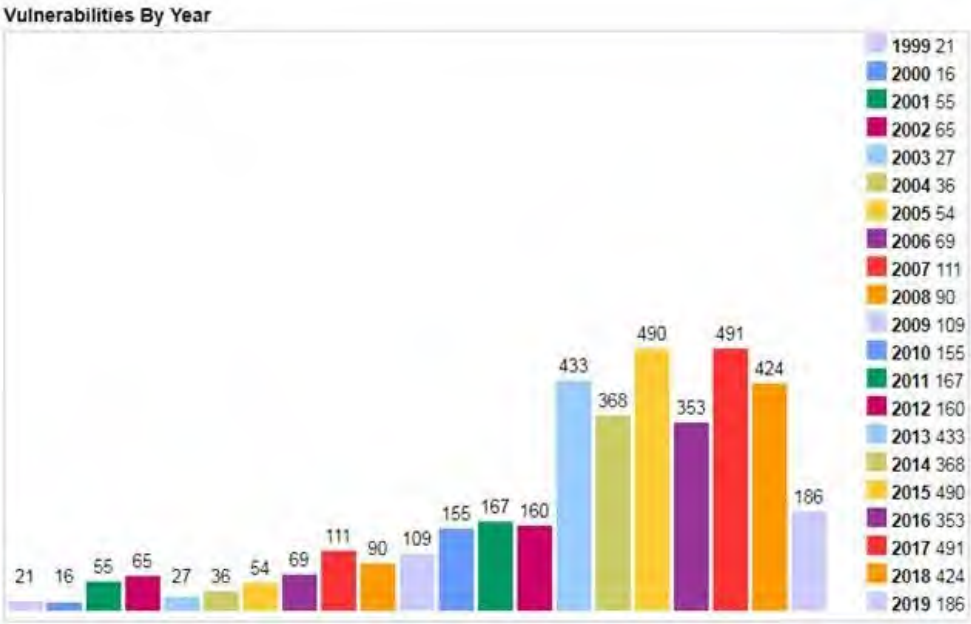
According to the number of vulnerabilities disclosed by the NVD, the Top 5 vendors are Microsoft, Oracle, Apple, IBM, and Google.

Vulnerability trends of Microsoft show that its number of vulnerabilities remains at a certain level. This shows on one hand Microsoft's continuous investment in security and on the other hand Microsoft's responsible disclosure of vulnerabilities. In addition, Microsoft uses the bug bounty program to encourage people to discover vulnerabilities.



Link: https://www.cvedetails.com/vendor/26/Microsoft.html

Cisco also has its own vulnerability disclosure channel. The number of vulnerabilities disclosed by Cisco also remains at a certain level.



Link: https://www.cvedetails.com/vendor/16/Cisco.html

3.4 Secure Coding Practices

3.4.1 Safe Function Analysis

The method used in the report to analyze safe functions has the following problems, which leads to inaccurate results:

1) The assessment does not cover a large number of safe functions in Huawei products, such as *VOS_MemCpy_Safe* and *VOS_nsprintf_Safe*, which causes serious deviation in the security assessment results.

2) Inaccurate understanding of unsafe functions

   (1) The report lists on page 33 some unsafe functions, including puts, memcmp, and asprintf.

   (2) As a memory clearing function, memset is used within Huawei to clear the newly applied memory and arrays with a fixed length. It has a very low risk. Even Microsoft that promotes safe functions does not have the corresponding safe function.

   (3) Functions such as fopen, access, system, remove, and execl must be used in code to meet service requirements. Using these functions does not necessarily lead to vulnerabilities.

3) Some functions in the report are regarded as both safe and unsafe.

   (1) asprintf is listed as an unsafe function in "Top 20 Most Commonly Used Unsafe Functions" on page 34, but is listed as a safe function later in "Safe and Unsafe Function Collections" on page 36. drv_cvb_memcpy_s_impl is listed as both a safe and unsafe function in "Safe and Unsafe Function Collections" on page 36 of the report.

   (2) According to "Top 20 Most Commonly Used Unsafe Functions", the author regards the execl function as unsafe but execlp, execv, execve, execvp, execle, and execvpe as safe, which is incorrect.

3.4.2 Compiler Security Option Analysis

In addition to RELRO, ASLR, DEP, and StackGuard mentioned in the report, at least three other compiler security options are important. In an embedded communications device, enabling compiler security options generally deteriorates product performance, even prevents product functions from running properly in some cases. It demonstrates the lack of maturity and competence of Finite State to comment on the enabling of compiler security options in embedded communications software from the perspective of general software only. Huawei would be happy to teach Finite State the basics of imbedded systems and global telecommunications operations that cover the globe.

Huawei has been carrying out in-depth researches on compiler security options for many years and attaches great importance to security. We will enable compiler security options as much as possible when conditions allow. As far as we know, Huawei leads the communications industry in terms of implementation in this regard.

Appendix: Introduction to the SCA Method of Finite State

Finite State uses the Software Composition Analysis (SCA) method in the assessment report, which is consistent with the industry. Many companies in the industry provide such an analysis service. The report of the research firm Forrester shows their SCA vendor evaluation, in which Finite State is not found. The Forrester Wave™: Software Composition Analysis, Q2 2019 link is :https://reprints.forrester.com/#/assets/2/230/RES146435/reports.

SCA Principles

Currently, the commonly used open-source software and vulnerability analysis technology SCA have two major purposes:

1) Identify the version and license information of the open-source software used to ensure compliant use.

2) Search the vulnerability library by open-source software version to obtain all vulnerabilities in the open-source software.

Source: blog of WhiteSource, a leading SCA solution provider according to Forrester

First and foremost, SCA tools generate an inventory report of all open source components in your products, including all direct and transitive dependencies. Taking inventory of open source usage is critical as it is the basis for properly managing your open source usage. After all, how can you secure or ensure compliance of something you do not know you're using?

Once all open source components have been identified, SCA tools provide information on each component. Basic information includes the open source license and whether there's a security vulnerability associated with that component.

The SCA method analyzes the firmware in the following steps:

1) Extract the complete hash value, partial hash value, function symbol name, file name, etc. of each binary file in the firmware as features. Identify the name and version of the open-source software referenced in the firmware based on these features.

2) On the basis of open-source software name and version information obtained in step 1, search the vulnerability library and obtain all vulnerabilities in the open-source software.

The SCA result is only an intermediate result and generally needs to be further confirmed with the firmware developer.

HUAWEI

Revision History: V1.1 UPDATED Add the link of the Software Composition Analysis from Forrester

Read our statement repudiating Finite State's report findings

Read our response to Nokia's accusations

in

Press & Events

News

Events

Huawei Facts

Annual Reports

Photo Gallery

Partners

Solution Partners

Channel Partners

Service Partners

Support

Consumer Support

Enterprise Support

Carrier Support

Security Bulletins

Portals

Careers

Developers

Suppliers

Huawei Blog

Others

Huawei Cloud

FusionSolar Smart PV

Huawei Marine

Honor Official Site

Exhibit 17

11/1/2019 Huawei Ex Parte
(providing an expert report on China's National Intelligence Law)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket. Huawei seeks to address concerns raised by the Commission regarding obligations that Chinese laws purportedly impose on Chinese companies. Specifically, the Commission has stated that it understands that Chinese law permits the Chinese government to "demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information." As support, the Commission points to Articles 7, 14, and 17 of China's 2017 National Intelligence Law.[1]

---

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Draft Report and Order, Order, and Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC-CIRC1911-01, para. 44 (circulated Oct. 29, 2019) ("Draft Report and Order")*; see also China Mobile International (USA) Inc., Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, ITC-214-20110901-00289 at para. 17 (rel. May 10, 2019)

Huawei has submitted substantial documentation into the record demonstrating that Chinese laws, including the National Intelligence Law, do not provide a mechanism through which the Chinese government can require Huawei to implant "backdoors" in its equipment or elsewhere, or otherwise assist the government with cyberespionage efforts.[2] Huawei has previously submitted an expert report by Dr. Hanhua Zhou, who clarified that any support, assistance, and cooperation obligations are strictly defensive and generally limited in scope by the Chinese constitution.[3] In doing so, Dr. Zhou provided detailed analyses of various provisions of relevant Chinese laws, including Articles 7 and 14 of the 2017 National Intelligence Law.

Huawei now submits as **Attachment A** the supplemental expert report of Dr. Hanhua Zhou,[4] which further analyzes obligations imposed on companies under Article 17 of China's National Intelligence Law. Dr. Zhou explains that Article 17 does not, as the Commission alleges, "allow[] Chinese intelligence agencies to take control of an organization's … communications equipment."[5] Article 17 provides for the staff of national intelligence agencies, when necessary to their work, to "have preferential use of, or [to] lawfully requisition, transport vehicles, communications tools, premises or buildings of relevant organs, organizations, and individuals"

(stating that the Commission understands Chinese law to "require citizens and organizations … to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world").

[2] *See, e.g.*, Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, at Exhibits D, E (filed June 1, 2018); Written Ex Parte Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, at Exhibits A, B (filed Aug. 6, 2018); Written Ex Parte Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89 (filed May 10, 2019) ("Zhou Initial Expert Report").

[3] Zhou Initial Expert Report. Dr. Zhou is a research scientist at the Institute of Law, Chinese Academy of Social Sciences.

[4] *See* Zhou Hanhua, "Expert Opinion on Article 17 of China's National Intelligence Law," (Oct. 31, 2019) ("Zhou Supplemental Report").

[5] *Supra* n.1.

and to "set up relevant work sites, equipment and facilities."[6] But neither clause allows an intelligence agency to take control of a company's telecommunications infrastructure. First, under Chinese law, the term "communications tools" refers only to mobile phones or pagers, and does not include telecommunications facilities such as switches, servers, and routers.[7] Second, the provision permitting staff to "set up relevant work sites, equipment, and facilities" does not impose any assistance obligations on third parties.[8] And even where the law permits preferential use of certain objects, it imposes no obligation to assist in any interception or monitoring of information.[9] In addition, Dr. Zhou clarifies that Article 17 is only applicable to the territory of China—and therefore has no bearing on Huawei's U.S. operations at all.[10] Nothing in the law or its application to Huawei in China allows intelligence officials to access telecommunications facilities, much less telecommunications facilities in *carriers' networks in the United States*, or entitles intelligence officials to Huawei's assistance in such an endeavor.

Dr. Zhou further clarifies that Article 17 is a defensive measure and does not provide authority for Chinese intelligence agencies to engage in offensive intelligence activities.[11] This is consistent with the generally defensive approach of the National Intelligence Law, as evidenced by Dr. Zhou's detailed analysis of multiple other provisions in his initial report. For example, Article 28 lays out liabilities for non-compliance with the National Intelligence Law. Importantly,

---

[6] National Intelligence Law of the People's Republic of China, Article 17; *see also* Zhou Supplemental Report at para. 1.

[7] Zhou Supplemental Report at para. 3.

[8] *Id.*

[9] *Id.*

[10] *Id.* at para. 4.

[11] *Id.*

parties are not necessarily subject to legal liabilities for mere non-compliance. Instead, the National Intelligence Law is concerned with parties who "obstruct" the law, a term that generally involves an intentional effort to hinder law enforcement through violence, threatening, or other acts.[12]

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, D.C. 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.

November 1, 2019

[12] *Id.* at para. 6.

Exhibit 17-A

Supplemental Expert Report of Dr. Hanhua Zhou

Expert Opinion on Article 17 of China's National Intelligence Law

Zhou Hanhua Research Scientist at the Institute of Law, Chinese Academy of Social Sciences (CASS)

As entrusted by Huawei, I have analyzed the foreign government's recent concern: "Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment." This relates to Article 17 of the National Intelligence Law of the People's Republic of China.[1] This Article stipulates that: "The staff of national intelligence agencies may, upon presentation of relevant identification, enjoy convenient travel as needed to carry out urgent tasks. To accomplish duties as required for their work, the staff of national intelligence agencies may, in accordance with relevant national provisions, have preferential use of, or lawfully requisition, transport vehicles, communications tools, premises or buildings of relevant organs, organizations and individuals. When necessary, they may set up relevant work sites, equipment and facilities. After the tasks are completed, these items shall be promptly returned, or restored to their original conditions, the corresponding fees shall be paid in accordance with provisions, and compensation shall be made where damages are caused."
In terms of the legal meaning of the above paragraphs and the several outstanding important issues related to them, I hereby give the following opinion:

1. Article 17 is divided into two paragraphs, which are applicable to different situations. The two paragraphs are distinctly different in nature and need to be interpreted separately.
2. Paragraph 1 stipulates that: "The staff of national intelligence agencies may, upon presentation of relevant identification, enjoy convenient travel as needed to carry out urgent tasks." This paragraph contains the following essentials: (1) These powers are awarded to the staff of national intelligence agencies, which are specific and do not include the staff of enterprises, public institutions, social organizations, or other state organs. (2) The prerequisite for applying this paragraph must be "as needed to carry out urgent tasks." It is generally understood that such tasks are not pre-planned, or even if they are pre-planned, they have become urgent tasks due to situation changes. Therefore, such tasks are urgent and sudden, and require emergency response. (3) The subjects of power shall present "relevant identification." Such identification is generally understood as a law enforcement document or a document proving that the subjects carrying out urgent tasks are "staff of national intelligence agencies." (4) The subjects of power "enjoy convenient travel." This means in general terms that the staff of national intelligence agencies, where feasible, have priority to use public transport vehicles such as planes, trains and cars, and are furthermore able to pass in the case of obstructed traffic. In certain cases, such convenient travel may also include exemption of tolls, parking fees and other fees when the staff use their own transport vehicles.[2] Beyond that, the subjects of power are not able to benefit

[1] See the *FCC Denies China Mobile Telecom Services Application* (FCC Denies International Section 214 Application of China Mobile USA; abbreviated as "FCC Denial Order" in this document).
[2] For example, according to the Notice of Yunnan Provincial Planning Commission on the Exemption of Fees for Parking in Parking Lots Invested by the State for State Security Organs Carrying Out Tasks in Yunnan issued on November 26, 2001, "pursuant to Articles 9 and 16 of the State Security Law and Articles 12 and 25 of the Rules for Implementation of the State Security Law", "parking lot management entities shall provide convenience as

from any advantages. (5) The subjects of obligation under this paragraph are limited to subjects that provide public transport vehicles, subjects that direct traffic, and subjects related to traffic and transport (such as places where vehicles are parked and toll stations). **The obligations of such subjects are limited to providing convenient travel and do not include any other obligations.**

3. Paragraph 2 stipulates that: "To accomplish duties as required for their work, the staff of national intelligence agencies may, in accordance with relevant national provisions, have preferential use of, or lawfully requisition, transport vehicles, communications tools, premises or buildings of relevant organs, organizations and individuals. When necessary, they may set up relevant work sites, equipment and facilities. After the tasks are completed, these items shall be promptly returned, or restored to their original conditions, the corresponding fees shall be paid in accordance with provisions, and compensation shall be made where damages are caused." Paragraph 2 contains the following essentials: (1) The subjects of power are limited to "the staff of national intelligence agencies." (2) The prerequisites for applying this paragraph must be "To accomplish duties as required for their work" and "in accordance with relevant national provisions." Paragraph 2 is applicable only when both prerequisites are met. Although no specific rules for implementing this paragraph have been issued, according to the general operating rules of Chinese law, "To accomplish duties as required for their work" indicates that a strict control procedure shall be made available within a national intelligence agency to determine duties which are applicable as work. A regular workforce is unable to decide such matters. "In accordance with relevant national provisions" means that implementation rules, as the basis for law enforcement, must be made public and not be held internally. Implementation rules are state-level regulations, and regional regulations are not allowed. Requirements such as entity conditions, permissions and procedures for initiating preferential use or lawful requisition shall be specified in the implementation rules, including safeguarding the rights of subjects of obligation to statement and to defend themselves. Compared with paragraph 1, paragraph 2 stipulates stricter conditions. It is impossible for the staff of national intelligence agencies to initiate the preferential use or lawful requisition procedure without fulfilling the prerequisite "upon presentation of relevant identification." (3) The subjects of obligation under paragraph 2 are defined as "relevant organs, organizations and individuals", which are different from the expressions in other relevant laws (such as "organs, organizations, enterprises, public institutions and individuals" in Article 11 of the Counterespionage Law, Article 13 of the People's Police Law, and Article 9 of the National Security Law (2009)). They are also different from the expression ("organs, organizations, enterprises, public institutions and individuals") in Article 15 of the draft National Intelligence Law. According to the systematic interpretation of laws and interpretation of the legislation history, paragraph 2 does not include the words "organizations, enterprises and public institutions", indicating that the legislative organ is more cautious about applying the measures in paragraph 2 to organizations, enterprises (including foreign investment enterprises), and public institutions. In practice, the measures may be applied more strictly or be restricted. Organs generally refer to state organs, and organizations have a broader meaning, including not only corporate organizations, such as enterprise legal

---

much as possible and exempt parking fees when provincial state security organs carry out tasks and park their cars with a local license in parking lots of airports, ports, wharfs, stations, stadium, shopping malls, parks, amusement parks, or other places invested by the state after showing a 'special pass' or 'secret pass with a car pattern'. Other parking lots shall also provide convenience for such state security organs."

persons, institutional legal persons and juridical associations, but also unincorporated organizations. Therefore, the subjects of obligation under this paragraph, if literally interpreted, should include organs, organizations, enterprises, public institutions and individuals in China (including foreign investment enterprises and foreigners in China). The scope of subjects of obligation under this paragraph and criteria for applying this paragraph to different subjects are uncertain and need to be verified in practice. (4) The power is limited to "have preferential use of, or lawfully requisition, transport vehicles, communications tools, premises or buildings of relevant organs, organizations and individuals." Accordingly, the subjects of obligation are obligated to transfer the rights of use and control of transport vehicles, communications tools, premises or buildings to subjects of power, and do not have any other obligations. **This is also the "administrative requisition" that is common in the laws of China and other countries where state administrative organs can temporarily obtain the right to use requisitioned property for public interests and public purposes, without transferring the property ownership. Administrative requisition is not exclusive to intelligence agencies.** For example, Article 44 of the Real Right Law stipulates that: "In case of emergent dangers or disasters, one is allowed to use the real properties or movable properties of entities and individuals in accordance with the statutory power limit and procedures." Article 15 of the Regulation on the Relief of Natural Disasters stipulates that: "During the emergency period for the relief of a natural disaster, the local people's governments at or above the county level or the emergency coordination bodies of the people's governments may requisition materials, equipment, transport vehicles and premises in their administrative regions, but shall return them immediately after the emergency rescue work is done and offer compensations pursuant to the relevant state provisions." Article 20 of the 2004 Amendment to the Constitution of the People's Republic of China revised Article 10(3) of the Constitution from "The State may, in the public interest, requisition land for its use in accordance with the law." to "The State may, in the public interest and in accordance with law, expropriate or requisition land for its use and make compensation for the land expropriated or requisitioned." Article 22 of the 2004 Amendment to the Constitution revised Article 13 of the Constitution from "The State protects the right of citizens to own lawfully earned income, savings, houses and other lawful property." and "The State protects according to law the right of citizens to inherit private property." to "Citizens' lawful private property is inviolable.", "The State, in accordance with law, protects the rights of citizens to private property and to its inheritance.", and "The State may, in the public interest and in accordance with law, expropriate or requisition private property for its use and make compensation for the private property expropriated or requisitioned." The Amendment to the Constitution clearly specifies "expropriated or requisitioned" objects as things or property, which do not have the obligation to act. Expropriation involves the transfer of ownership, whereas requisition does not. This amendment is clearly and consistently reflected in other relevant subsequent laws. For example, Article 117 of the General Provisions of Civil Law stipulates that: "Fair and reasonable compensation shall be paid if any real properties or movable properties are expropriated or requisitioned for public interests, according to the authority and procedure as prescribed by the law." This reflects the difference between expropriation and requisition in the nature of law: expropriation involves the transfer of ownership, whereas requisition does not. In addition, expropriated or requisitioned objects are limited to "real properties or movable properties" and do not involve the obligation to act. The

National Intelligence Law shall also be interpreted within the constitutional framework. The obligation boundaries of paragraph 2 in Article 17 can therefore be clearly defined. First, the obligations are limited to four types of objects, namely, transport vehicles, communications tools, premises and buildings, which all belong to "things" of the subjects of obligation. **These objects do not involve the behavior of the subjects of obligation and do not include objects not specifically listed, such as business secrets, business information, and communications information attached to communications tools.** Second, "preferential use" or "lawful requisition" only temporarily transfers the rights of use and control of these things during the period when the staff of national intelligence agencies carry out tasks. **The staff of national intelligence agencies can control and use these things, but the ownership remains unchanged. Besides the temporary transfer of the rights of use and control, the owners and operators (subjects of obligation) are not obligated to provide other intelligence law enforcement cooperation (except normal O&M obligations to maintain these things). For example, the owners and operators are not obligated to assist in interception/monitoring or information acquisition.** Although the Constitution does not explicitly define "preferential use", the objects can only be things rather than behavior, according to normal understanding in Chinese. The provisions of "promptly returned" and "restored to their original conditions" in this paragraph also indicate that the objects can only be things rather than behavior. In addition, each type of object is specific and has the characteristic "immediate return after use" of things, so that the objects can be "promptly returned" or "restored to their original conditions." **For example, it should be emphasized that the term "communications tools" in Article 17 of the National Intelligence Law refers to "tools" rather than "facilities"; however, the FCC Denial Order incorrectly translated this term into "communications equipment." According to relevant Chinese laws involving "communication tools"[3], "communication tools" refer to mobile phones or pagers, rather than telecommunications facilities such as switches, servers, and routers.** (5) According to the preceding reasoning, after the staff of national intelligence agencies obtain the rights to temporarily control and use any type of the objects, they may "set up relevant work sites, equipment and facilities" on the objects "when necessary", which is a subordinate and subsidiary authority not requiring separate authorization. Even if authorized, no new authority will be generated, and no new obligations will be incurred for third parties. The subjects that "set up relevant work sites, equipment and facilities" are still the staff of national intelligence agencies rather than third parties, and third parties cannot be required to perform assistance obligations. (6) After completing the tasks, the staff of national intelligence agencies shall return the objects promptly, or if any object is changed, restore the object to its original condition, with the expenses for the use or requisition to be paid in accordance with provisions. The FCC Denial Order uses Article 17 of China's National Intelligence Law as an example and raises its concern about the security risks brought by Chinese intelligence agencies' control over communications equipment in organizations to the U.S. This is an incorrect interpretation of the Article. First, the staff of national intelligence agencies have transferred the rights of control and use of an object back to its owner or operator

[3] Article 29 of the Regulation of the People's Republic of China on Flood Control (2011), Article 29 of the Notice of the All China Lawyers Association on Issuing the Rules on the Handling of Criminal Cases by Lawyers (Provisional) (1997), Article 2 of the Provisional Regulation on Determining the Price of Property Involved in Cases of Discipline Inspection and Supervision Organs (2010), Article 6 of the Regulation on Handling Major Animal Epidemic Emergencies (2006), and more

after they promptly return the object or restore it to its original conditions. Second, enterprises can decide not to sell or provide the communication tools that have been requisitioned to customers to avoid the possible compromise of customers' communications security. (7) The objects are lawfully used or requisitioned. Therefore, compensation shall be made according to law if any loss is caused to the objects in the preferential use or lawful requisition.

4. Article 17 is applicable only to the territory of China. The reasons are as follows: (1) The Instructions on the draft of National Intelligence Law of the People's Republic of China specifies that: "Foreign bodies, organizations or individuals who engage in acts that endanger the national security and interests of China within Chinese territory must face legal punishment. National intelligence agencies shall provide intelligence as a reference or basis for preventing, curbing and punishing such acts." "The staff of national intelligence agencies may, when lawfully exercising their duties, acquaint themselves with the relevant organs, organizations, enterprises, public institutions and individuals. Moreover, they reserve the right to inquire into relevant circumstances, consult or obtain relevant files, materials and goods, enter relevant limited-access areas and premises, and enjoy convenient travel."[4] A literal interpretation indicates that the above mentioned measures are only allowed within Chinese territory. In addition, these measures are taken for "preventing, curbing and punishing the acts" that "endanger the national security and interests of China." These acts are defensive, and do not authorize national intelligence agencies to engage in offensive intelligence activities.[5] (2) According to Article 16 ("with permission and after presenting relevant identification, enter relevant limited-access areas and premises") and Article 18 ("may request customs, exit/entry border inspection authorities and other such bodies to provide exemption from inspection and other convenience"), the acts are applicable only within Chinese territory. This means that the staff of national intelligence agencies cannot enter limited-access areas and premises after presenting identification outside of China, or ask customs and border inspection authorities to provide convenience from outside of China. Therefore, according to the systematic interpretation of laws, Article 17 is applicable only within Chinese territory. (3) Article 16 of the draft National Intelligence Law[6] stipulates that: "The staff of national intelligence agencies may, when lawfully exercising their duties according to relevant national regulations, with permission and after presenting relevant identification, enter relevant limited-access areas and premises; they may, upon presentation of relevant identification, enjoy convenient travel as needed to carry out urgent tasks. As is necessary for their work, the staff of national intelligence agencies may, in accordance with relevant national provisions, have preferential use of, or lawfully requisition, the transport vehicles, communications tools, premises or buildings of organs, organizations, enterprises, public institutions and individuals. When necessary, they may set up relevant work sites, equipment and facilities and once the tasks are completed, these items shall be promptly returned, or restored to their original conditions, while the

[4] Chen Wenqing, Minister of State Security of the People's Republic of China, *Instructions on the National Intelligence Law of the People's Republic of China (Draft)*, at the 25th Session of the Standing Committee of the Twelfth National People's Congress on December 19, 2016.

[5] For a comprehensive analysis of the defensive and reactive nature of legal obligations under China's national security laws, see: Zhou Hanhua, *On the Nature of Legal Obligations Under China's National Security Laws: Based on Comparison of Chinese and Australian Laws*, Peking University Law Journal, No. 4 (2019) p. 871-890.

[6] The 25th Session of the Standing Committee of the Twelfth National People's Congress reviewed the *Instructions on the National Intelligence Law of the People's Republic of China (Draft)* and issued the Draft at the official website of the National People's Congress of the People's Republic of China to solicit public opinions.

corresponding fees shall be paid in accordance with the necessary provisions, and compensation shall be made where damages are caused." Articles 16 and 17 in the National Intelligence Law were in the same article, indicating that they are applicable to the same scope mentioned above. (4) No extraterritorial effect is specified for the National Intelligence Law. This Law is effective only within Chinese territory, and does not require subjects outside of China to fulfill legal obligations according to Chinese law.

5. Implementation assurance mechanisms for Article 17. The National Intelligence Law provides at least four mechanisms to ensure strict compliance with Article 17 and other provisions. (1) Article 19 stipulates that: "National intelligence agencies and their staff shall act in strict accordance with the law and must not exceed or abuse their powers, infringe on the legitimate rights and interests of citizens and organizations, use their position to facilitate personal gains for themselves or others, or disclose state secrets, business secrets and personal information." This is a typical preventive and detective control mechanism for codes of conduct that prevents acts beyond one's authority and abuse of one's authority from occurring. (2) Article 26 stipulates that: "National intelligence agencies shall establish and implement a strict supervision and security review system, supervise their staff's compliance with laws and disciplines, and take necessary measures according to the law to conduct security reviews on a regular or irregular basis." This is a typical top-down proactive review control mechanism, which is initiated by national intelligence agencies. (3) Article 27 stipulates that: "Any individual or organization shall have the right to prosecute or accuse national intelligence agencies and their staff of any abusive conduct and other law violating acts. The relevant authorities accepting the prosecution or accusation shall promptly investigate it and inform the prosecutor and accuser of the result of the investigation. Furthermore, no individual or organization may suppress or retaliate against individuals and organizations that have prosecuted or accused national intelligence agencies and their staff. National intelligence agencies shall provide convenient channels for individuals and organizations to prosecute, accuse, and report instances of abuse and law violation, while keeping details of the prosecutor and accuser confidential." This is a typical external prosecution and accusation supervision mechanism, which enhances the supervision of intelligence activities through external participation. (4) Article 31 stipulates that: "National intelligence agencies and their staff who have exceeded or abused their powers, infringed on the legitimate rights and interests of citizens and organizations, used their position to facilitate personal gains for themselves or others, or disclosed state secrets, business secrets and personal information shall be punished according to law. If the act constitutes a crime, criminal liability shall be pursued according to law." This is a post-event legal accountability mechanism, which regulates the activities of intelligence agencies by lawfully enforcing deterrent penalties. In addition to the four mechanisms, it is equally important that, according to the Administrative Reconsideration Law and Administrative Procedure Law, the subjects of obligation who consider that administrative acts, such as the preferential use or lawful requisition, of national intelligence agencies infringe upon their legitimate rights and interests or who believe that their transport vehicles, communications tools, premises or buildings shall not be preferentially used or lawfully requisitioned may apply for administrative reconsideration or file administrative proceedings according to law. The National Intelligence Law does not explicitly define remedy mechanisms such as administrative reconsideration and administrative proceeding. This does not indicate that these mechanisms are excluded from application.

6. Legal consequences of failure to comply with the obligations under Article 17. The National Intelligence Law does not explicitly define the legal liability of the subjects of obligation who fail to fulfill the provisions in Article 17. However, Article 28 of the Law stipulates that: "Where provisions of this Law are violated by obstructing national intelligence agencies and their staff from lawfully carrying out intelligence work, the national intelligence agencies are to recommend relevant units to give out sanctions, or national security organs and public security organs are to give warnings or up to 15 days of detention; where a crime is committed, criminal liability shall be pursued according to law." Therefore, in the course of fulfilling the obligations under Article 17, if "obstruction" occurs, the subjects of obligation shall bear the administrative legal liability and criminal legal liability prescribed in this Article. The National Intelligence Law and Public Security Administration Punishment Law do not specify or list the circumstances that constitute "obstruction" in the sense of administrative violations. In the Chinese language and Chinese law, "obstruction" generally involves an intentional effort to hinder law enforcement through violence, threatening or other acts. Therefore, not all actions or omissions that fail to fulfill the legal obligations under Article 17 in a timely and comprehensive manner are regarded as "obstruction." If the rights of control and use of the four types of objects are not transferred in a timely and comprehensive manner due to objective reasons, this does not constitute "obstruction." Administrative legal liability cannot be pursued in accordance with Article 28 where the failure to fulfill legal obligations does not constitute "obstruction." In addition, according to the principle of no penalty without a law, any criminal liability to be pursued in China must be found in the Criminal Law. Slip laws including the National Intelligence Law cannot directly establish a crime or provide for criminal liability. Failure to fulfill the obligations under Article 17 is most likely to trigger the crime of obstructing public affairs as stipulated in Article 277 of the Criminal Law. Article 277(1) of the Criminal Law stipulates that: "Whoever uses violence or threatening to obstruct state personnel from performing their duties in accordance with the law is to be sentenced to no more than three years of fixed-term imprisonment, criminal detention or control, or a fine." Article 277(3) stipulates that: "Whoever intentionally obstructs national security organs or public security organs from carrying out their national security assignments, and has caused serious consequences even though no violence or threatening has been used is to be punished in accordance with the first paragraph." According to paragraph 1 of this Article, the premise for determining whether a crime is committed must be "administration according to law." A clear scope for the execution of public affairs must be specified; for example, lawful requisition refers to "discharging their duties according to law." If an enterprise is required to assist in building backdoors, this goes beyond the provisions of Article 17 in the National Intelligence Law and is not interpreted as "discharging their duties according to law." Additionally, "obstruction" must be specific, rather than general support or assistance obligations. China's Criminal Law has no charges or provisions regarding criminal liability for failing to fulfill the obligation of intelligence cooperation. In the Criminal Law, only Article 111 "Whoever steals, secretly gathers, purchases, or illegally provides state secrets or intelligence ..." defines intelligence-related crimes; however, this is not applicable to the failure to fulfill the obligation of intelligence law enforcement. If enterprises do not build backdoors, they will not be considered as specific obstructions, and consequently there is no legal basis for separately pursuing criminal liability.

7. With regard to the issue of lawyers' participation, according to the *General Office of the Central Committee of the Communist Party of China and the General Office of the State Council Issuing the Opinions on Promoting the Legal Adviser System and the Government Lawyer and Corporate Lawyer System* (June 16, 2016), by the end of 2017, all departments and commissions of the CPC Central Committee and state authorities, and local CPC and government departments at and above the county levels shall universally establish positions of legal advisers and government lawyers. Legal advisers refer to the staff who engage in legal affairs with the CPC and government departments as well as legal experts and lawyers who are employed by these departments. The responsibilities of legal advisers include but are not limited to: providing legal advice for major decision-making and administrative actions, and providing legal services for handling legal cases, petition cases, and major emergencies. Government lawyers are government officials of the CPC and government departments who have obtained a government lawyer certificate in accordance with national provisions. Government lawyers have the right to meet, consult case files, investigate, collect evidence and pose questions, cross-examine, and argue as well as other rights in practice activities as stipulated in the Lawyers Law. Therefore, in the above mentioned implementation assurance mechanisms of Article 17, it is necessary to involve legal advisers and government lawyers of intelligence agencies. Major law enforcement decisions of national intelligence agencies, including "administrative expropriation and requisition", must also go through verification by the legal review system defined in the *Guiding Opinions of the General Office of the State Council on Comprehensively Implementing the Administrative Law Enforcement Publication System, the Recording System of Law Enforcement in the Whole Process and the Legal Review System of Major Law Enforcement Decisions* (General Office of the State Council No. [2018] 118). Decisions that fail or do not go through legal review shall not be made. Both legal advisers and government lawyers will play an important role in the review process. Therefore, the notion that lawyers do not participate in China's intelligence work is not substantiated. Additionally, the subjects of obligation under Article 17 may also employ lawyers to provide relevant legal services in different phases in accordance to China's Lawyers Law, and there is no legally restrictive provisions or other legal impediment. Legal services offered by lawyers include: (1) serve as a legal adviser in administrative procedures, such as the preferential use or lawful requisition of objects, to provide non-litigation legal services, answer inquiries concerning law, and represent clients in writing documents regarding legal matters; (2) serve as an agent if a subject of obligation decides to apply for administrative reconsideration or bring an administrative lawsuit against the decision of the preferential use or lawful requisition of objects, or if the subject of obligation is given warnings or up to 15 days of detention by national security organs or public security organs in accordance with the National Intelligence Law; (3) accept authorization by a criminal suspect or defendant or accept appointment by a legal aid agency according to law to act as a defendant and participate in proceedings if criminal liability is pursued according to law.

I declare under penalty of perjury under the laws of the United States of America that the forgoing is true and correct.

Hanhua Zhou

Executed on Oct 31, 2019
Beijing, PRC

Exhibit 18

11/1/2019 Huawei Ex Parte
(providing an expert report on 5G network security)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket.

Huawei submits as **Attachment 1** the expert report of Professor Valtteri Niemi,[1] which analyzes how security is addressed in 5G network standards. Huawei understands and commends the U.S. Government's efforts to mitigate cybersecurity risks in its telecommunications infrastructure. However, as Huawei has explained extensively in the record, the Commission's proposed rule would harm a substantial number of carriers—and in particular carriers in rural and remote areas. The Commission is obligated to weigh carefully the costs and benefits of its proposed rule. In doing so, the Commission should take into account the enhanced security requirements and features built into the standards for 5G networks. For example, a recent report about 5G

[1] *See* Valtteri Niemi, "Expert Report on 5G Security," (Nov. 1, 2019) ("Niemi Report"). Professor Niemi leads the Secure Systems Research Group and serves as Deputy Head of the Computer Science Department at the University of Helsinki.

cybersecurity recognizes that "5G technologies and standards could improve security compared to previous generations of mobile networks, due to several new security functions, such as stricter authentication processes in the radio interface."[2] Moreover, "contingency approaches have been defined through standardization level by 3GPP" to mitigate many of the "identified risks" linked to 5G technology.[3] Proceeding to adopt the proposed rule, which does not account for the unique security features of 5G networks, would be arbitrary and capricious.

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, D.C. 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.

November 1, 2019

---

[2] *See* NIS Coordination Group, "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks: Report," para. 1.18, (Oct. 9, 2019), available at: https://g8fip1kplyr33r3krz5b97d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf.

[3] *Id.*, para. 3.7.

Exhibit 18-A

Expert Report of Professor Valtteri Niemi

Expert report on 5G security

Personal Background and Qualifications

I am a Professor of Computer Science at University of Helsinki where I lead the Secure Systems research group and am the Deputy Head of the Computer Science Department. Prior to my work with the University of Helsinki, I was a Professor of Mathematics in two other Finnish universities: (1) University of Vaasa from 1993 until 1997 and (2) University of Turku from 2012 until 2015. I also served for 15 years in various roles at Nokia Research Center and was nominated as a Nokia Fellow in 2009. At Nokia, I worked on various wireless security topics. I participated in the 3GPP SA3 security standardization group from its beginning and served as chairman of the group from 2003 until 2009. I have published more than 80 scientific articles and am a co-author of four books about mobile communications security.

A complete statement of my qualifications is set forth in my curriculum vitae, attached hereto as Exhibit A.

I have prepared this report at the request of Huawei Technologies Co. Ltd. and Huawei Technologies USA, Inc. (collectively, "Huawei"). This report represents my independent assessment and opinions.

Introduction

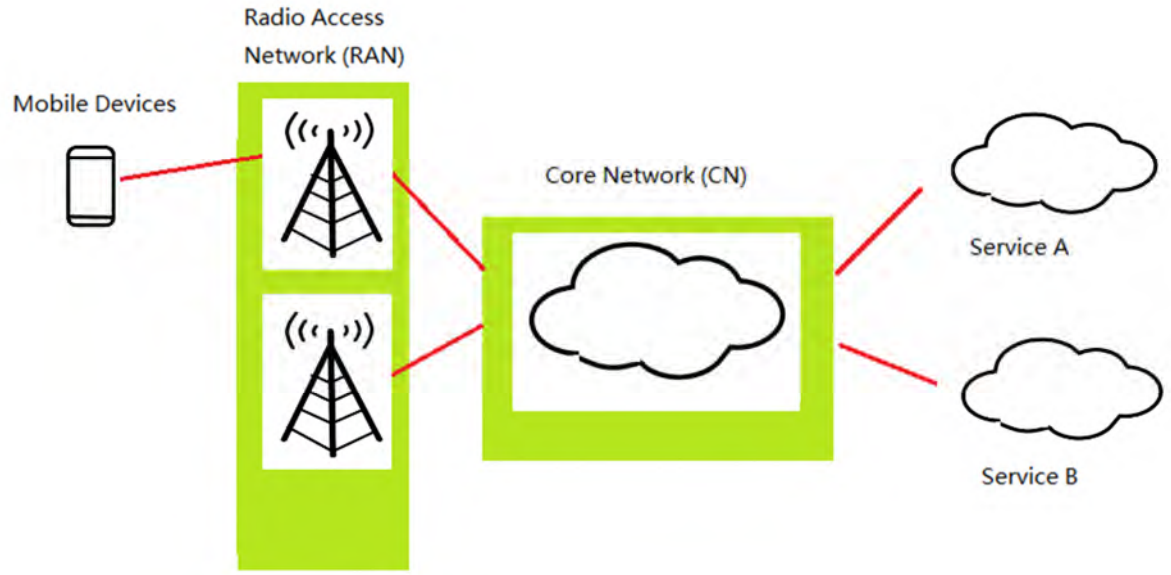
In considering adoption of rules that would prohibit the use of universal service funds for the purchase of equipment or services from providers identified as posing a national security risk to telecommunications networks, the Federal Communications Commission ("FCC") should consider how security will be addressed in 5G networks.[1] As this report explains, security has been a central topic in the development of 5G standards. As a result, those standards build in not only the security requirements and features of today's fourth generation wireless networks, but also additional requirements that will enhance security. Furthermore, those standards also reduce the likelihood for telecommunications networks to be subject to attack by bad actors.

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

5G basics

The term 5G refers to the 5th generation of mobile communication technologies. A mobile network contains both a network of base stations called the radio access network (RAN) and a core network (CN). Mobile devices communicate with base stations through radio links, and base stations connect with the CN typically by a wired link, although some may connect via wireless technologies. In mobile networks, the RAN equipment is often supplied by a different vendor than the CN equipment. The CN contains elements that are responsible for keeping track of the whereabouts of mobile devices, setting up calls, storing information about user subscriptions, managing base stations, authentication, charging and billing, and many other functions. The manufacturer of any element in the network does not take part in the operation of the element unless there is a specific agreement about such an arrangement between the network operator and manufacturer.

For each of the generations of wireless network technology prior to 5G, several different standardized technologies were created and deployed. However, one technology, referred to as Long Term Evolution (LTE), is clearly dominant in the 4th generation. The LTE standards were created by an organization that consists of seven different regional telecommunications standard bodies referred to as the 3rd Generation Partnership Project or 3GPP.[2] With respect to 5G, 3GPP has already developed the first standards applicable to this new technology, and current 5G deployments are based on these 3GPP standards. The standards keep evolving with advanced features and performance.



[2] *See* Introduction of 3GPP Organizational Partner, available at: https://www.3gpp.org/about-3gpp/partners.

The scope of 5G can be understood at least in three different ways. The narrowest view is to look at the way in which a mobile device, such as a smart phone or a tablet, communicates wirelessly with a base station. The 3GPP adopted a new radio interface called 5G New Radio (NR). It enables significantly higher bit rates than what can be provided by LTE technology.

A broader view of 5G considers the whole system. The first 5G deployments, appearing in several countries during the first half of 2019, follow a model where the existing LTE network is extended with 5G NR base stations. This model is referred to as 5G Non-Standalone (5G NSA) because it relies on the LTE core network and NR base stations are added into the RAN. The 3GPP has also developed specifications for a whole new core network, and in the 5G Standalone (5G SA) model, 5G NR base stations are connected to the 5G core network.

Finally, the broadest view of 5G is to consider all the different applications and services that would use 5G technologies in some manner. The commonly shared vision for 5G is that it would be used extensively for a much wider set of services than LTE. Examples of such services are ones needed for smart cities and for controlling robots in a factory. 3GPP has identified two main domains for new services: first, a Massive Internet of Things (MIoT); and second, Ultra Reliable and Low Latency communications (URLLC). The main characteristic of MIoT is the presence of a huge number of devices that are connected to a larger private network or public network, *i.e.*, the internet. The domain of URLLC supports use cases such as autonomous vehicles where communication has to be very reliable, the speed at which data traverses a network must be very fast, and the latency must be very low.

As with prior generations such as LTE, users of 5G networks create subscriptions with home networks. Home networks can have roaming agreements with other networks. Roaming agreements allow users to seamlessly create trust relationships with other networks when travelling outside users' home networks' coverage areas into coverage areas of these other networks.

In this report, I discuss security aspects for each of the three different viewpoints of 5G.

Overview of 3GPP work

The 3GPP specifications are developed by the international telecommunications industry and government players, with wide participation from all areas of the mobile communications ecosystem. Mobile network providers such as Verizon and China Mobile, network equipment vendors such as Ericsson and Huawei, mobile device vendors such as Apple and Samsung, and chipset vendors such as Qualcomm and Intel, are all contributing to these specifications, together with telecommunications regulators such as the FCC and representatives of vertical industries that plan to utilize these

technologies. Participants through October 28, 2019, include 686 individual member companies[3] across 45 countries and 18 organizations representing different segments of the telecommunications marketplace.[4]

3GPP is widely recognized as a successful and influential standards-setting organization. Since its establishment 20 years ago, working procedures of 3GPP have remained stable with only minor revisions. 3GPP aims for open and fair technical discussions, and its basic principle for reaching agreement is by consensus. The 3G and 4G standards developed by 3GPP have been widely deployed in the world. There is a high likelihood that the 5G standard developed by 3GPP will be the only 5G standard in the world, and a number of telecommunications companies are deploying 5G based on specifications provided for in 3GPP's first release (Release 15).

The working group SA3 is responsible for security technologies in 3GPP. There are more than 50 companies participating in SA3 meetings and more than 100 experts jointly worked on the 5G security standard by participating in the meetings, with many more experts contributing to the work from company offices. Key players in SA3 include Apple, AT&T, Ericsson, Huawei, Nokia, Qualcomm, Samsung, T-Mobile, and Vodafone, among others.

The first 5G security standard is associated with 5G Release 15 and provides the standardized security solutions for the features included in the first phase of 5G. Prior to the creation of the 5G security standard, the working group SA3 carried out an extensive study phase identifying key security issues as well as consideration of potential solutions to resolve identified vulnerabilities associated with the technology and the corresponding standards. The security standard continues to evolve in Release 16 and onwards to address new and additional security vulnerabilities attendant to the introduction of the new features and functionalities enabled by each 5G Release. For example, 5G enables new use cases for mobile networks and devices based on the capabilities of MIoT and URLLC. The potential vulnerabilities associated with these use cases require evaluation and consideration on an ongoing basis.

Security for 5G Non Standalone

In all generations of mobile networks, starting from GSM, certain important security features have been included and embedded in the radio level procedures. For example, encryption of the communication is handled between the mobile device and the RAN. The encryption is based on a shared secret key. This key is generated during the process whereby the mobile device and the mobile network authenticate each other. The core network is responsible for the authentication and key agreement procedure. After the key is generated, the core network sends it to the RAN. The mobile device is able to generate the same key based on the data it receives from the network, during the authentication procedure. These

[3] *See* 3GPP Membership, available at: https://webapp.etsi.org/3gppmembership/Results.asp?Member=ALL_PARTNERS&SortMember=Name&DirMember=ASC&SortPartner=Name&DirPartner=ASC&SortMarket=Name&DirMarket=ASC&SortObserver=Name&DirObserver=ASC&SortGuest=Name&DirGuest=ASC&Name=&search=Search.

[4] *See* 3GPP Market Representation Partners, available at: https://www.3gpp.org/about-3gpp/partners.

principles have been followed for 3G and 4G technologies, and the same is true for 5G. Therefore, security for 5G New Radio is very similar to LTE radio security.

There are differences in the specifics as to how encryption between the device and the network occurs in a 5G-based network compared to one based on 4G or 3G technologies due to the details associated with the different technological environments that devices and networks operate in based on these differing technologies. However, the overall principle of using encryption to transmit information between the device and network (and *vice versa*) and authentication procedures is similar across all technologies.

Starting with LTE, radio base stations have been sometimes placed in vulnerable locations where they are exposed to potential intruders, e.g., unsecured indoor locations or on roof-tops. As a result, LTE security solutions included platform security measures to protect base stations. Similar protection methods apply to 5G NR. It is important to note, however, that it is not possible to influence the authentication procedure by penetrating base stations, no matter whether the network in question is a 4G or 5G network. Moreover, 5G networks are designed to be resilient so that even if a base station is damaged or otherwise unable to operate the rest of the network is still able to function normally.

In summary, security for 5G New Radio is a result of a fairly straight-forward modification of LTE radio security. Because the 5G NSA system is formed by just adding 5G NR base stations to a LTE system without replacing the core network, the security of 5G NSA is very similar to that of the LTE system.

Security for 5G networks

The main part of the 5G authentication procedure between the mobile device and the network is identical to the corresponding procedure in LTE networks. However, the 5G authentication procedure includes an important additional feature. When operating in a 5G environment, home networks, in roaming situations, verify to ensure that roaming partner networks actually execute authentication procedures as expected. This new functionality assists 5G providers in offering users a more secure operating environment even when roaming.

As briefly described above, authentication is inherently tied with generation of secret keys. Starting with GSM, in all mobile networks, the master shared key for each user is stored in a tamper-resistant module that is called a SIM card for GSM. The corresponding module for 3G networks, LTE networks and 5G networks is called a Universal Integrated Circuit Card (UICC). In 5G networks, as in LTE networks, another key is derived from the above mentioned key to be used as a local master key in the visited network. From this derived master key, many more keys are derived, e.g., a different key for each base station. In 5G, the number of different types of keys that various network elements share with the mobile device is higher than in LTE networks. This provides support for more flexible network configurations and enhanced security. The security is enhanced in 5G networks as compared to earlier generations of mobile networks because in each context a separate key is in use, and it is not possible to derive any other key from one such key. Hence, even if one key is compromised, other keys remain

secure thereby limiting vulnerabilities to fewer devices and also requiring multiple layers of penetration by attackers.

5G networks also enhance security associated with user identities transmitted over such networks. Starting with GSM, and in all subsequent mobile network generations, user identities have been protected against potential radio eavesdroppers. These kinds of attackers would tune in to the radio frequencies reserved and licensed for mobile communications. Such attackers cannot determine users' identities because the network employs the use of temporary identities, i.e., pseudonyms, for users and transmits information about pseudonyms over encrypted channels. Eavesdroppers cannot decrypt the protected information because they do not know or otherwise have access to the shared key. However, in mobile networks that pre-date 5G, determining users' identities is possible for sophisticated attackers. In contrast, public key cryptography is used in 5G to prevent a rogue base station from obtaining a user's permanent identity. This is because a user's permanent identity is always delivered in encrypted form, and only the user's home network can decrypt the identity. The home network provides later the decrypted permanent user's identity to a serving network.

The 5G core network allows access for users through technologies other than 5G New Radio. Other radio interfaces defined by 3GPP, such as LTE or 3G, are supported, as well as access via Wi-Fi or other technologies that are not defined in 3GPP. Regardless of the technology used to access the 5G core network, 5G networks employ a unified authentication framework. For example, it is possible to derive a shared key usable over a Wi-Fi connection from the local master key allowing for the secure exchange of information between the Wi-Fi connection and the 5G network.

The Cloud is one of the key technologies influencing the 5G core network, and to some extent the 5G RAN in some deployment scenarios. Instead of relying on full-featured devices, 5G networks allow for implementing various functions as software on top of general-purpose hardware, typically residing at the data center level. In this way, the network becomes more flexible. This approach is called Network Function Virtualization (NFV). The virtualization approach for the 5G core network has been taken into account beginning already in the design phase for 5G. One result of NFV is the ease of adding new functions to the 5G core network that has a Service-Based Architecture (SBA) compared to LTE that employs a traditional network architecture. In the SBA setting, in order to add a new network function, it is sufficient to define how other functions can make requests to the new function and how the new function would respond to those requests. In contrast, if a new network function is added to the traditional network architecture, one typically needs to define different interfaces from the new function towards all such existing network functions with which the new function may need to communicate. This is done in order to allow the new functions to cooperate with the existing functions in the network architecture.

The SA3 working group has specified a security solution for SBA. The key component of the solution is inclusion of a Security Edge Protection Proxy (SEPP). This proxy acts as a gate-keeper for the network and transmits over a secure channel with similar proxies on other networks, which arrangement is needed and applicable for users roaming on third-party service provider networks. Mobile networks that preceded 5G have been found to be vulnerable to attacks in roaming environments where attackers

could manipulate third party devices controlled by roaming carriers. Accordingly, as compared to earlier generations of mobile networks, 5G is more secure due to SBA SEPP preventing these and similar attacks from tampering with critical data that is exchanged between core networks.

One aspect that is carried over from LTE security procedures to 5G is the functional split of RAN and the CN. The key security functions, i.e., authentication, access control, subscriber identity privacy and lawful interception, reside on the CN rather than on the RAN. The inclusion of Multi-Access Edge Computing (MEC) as a core network function according to the 3GPP specification in Release 15 sometimes causes confusion with respect to the functional security split between RAN and the CN. The MEC functionality, defined as a core network function according to the 3GPP specification, enhances applications' responses to users by enabling such functionality at locations geographically closer to users at the edge of the core of the 5G network. However, the edge of the network in this sense is the edge of the external data network, not the edge of the mobile network and this does not change the functional split between the RAN and the core network. Thus, the security arrangements associated with the functional split of RAN and CN remains in place in 5G networks.

In conclusion, security procedures for 5G networks are consistent with principles of LTE network security but are also enhanced and extended in several important ways that make 5G networks inherently more secure than prior generations of mobile networks. Several new security mechanisms have been introduced while no security mechanisms that exist in the LTE network architecture have been discontinued.

Security for services that use 5G networks

When 5G is interpreted broadly to include all services and applications that utilize 5G networks and technologies, 3GPP's Release 16 addresses a wider scope of security issues than those covered by Release 15. These service-specific security issues are beyond the scope of this report, though required security solutions for all Release 16 features will be defined by 3GPP's Release 16. Moreover, 3GPP can provide generic enablers and standards that may be useful for many services that deal with massive IoT or URLLC. Several studies have already been carried out in the SA3 working group about key security issues in these domains and potential solutions. 3GPP has enabled network players to take care of the security of the wireless communication network itself. The additional service and application security, however, is the responsibility of application and service providers. For example, the application provider is responsible for encryption in the application layer. Through end-to-end encryption enabled by the application provider, information sent by a user is encrypted from its source (i.e., the user sending out the information using the application), with decryption only taking place at the information's destination (e.g., another user receiving the information using the same application).

Security for 5G deployments

In addition to effective security standards built into the 5G standards, it is important to test products against the standards to assure that implementation is aligned with the standards. The SA3 working group has created many specifications that can be used to verify whether implementations of security features operate as intended. This is called security assurance work. There are separate specifications for all different elements in the network.

The GSM Association (GSMA) also has established the Network Equipment Security Assurance Scheme (NESAS) for the purpose of security test work. The 3GPP expects to publish the first version of the relevant standards in 2019. The draft version is under review by all stakeholders including regulators from key countries including the United States. 3GPP approved the Security Assurance Specification (SCAS) for 5G base stations in June 2019, and corresponding SCAS specifications for core network functions were approved in September 2019.

There are also other activities on this front. For example, an industry forum Next Generation Mobile Networks (NGMN) plans to establish a lab for 5G security testing work.

Conclusions

As this report notes, there are several different perspectives on 5G security. The first viewpoint concerns the new radio interface. As I have explained in this report, security for 5G New Radio is a result of a fairly straight-forward modification from LTE radio security. Because the 5G Non-Standalone system is formed by just adding 5G New Radio base stations to an existing LTE system without replacing the core network, the security of 5G Non-Standalone is very similar to that of the LTE system.

The second viewpoint is for the new core network. As I have explained in this report, security procedures for 5G core networks are consistent with principles of LTE network security, but are also enhanced and extended in several important ways. The functional split between the RAN and the core network for key security functions such as authentication remains for 5G networks, while additional mechanisms such as the use of many security keys meaningfully enhance the security of 5G networks.

The third viewpoint is about the 5G service ecosystem. The 3GPP has enabled network players to address the security of the network itself. Additional service and application security is taken care of by application and service providers.

There is also the matter of 5G deployments. Several activities have been established by different parties for providing assurance of appropriate security measures in products and deployments in compliance with 3GPP's 5G standards.

Exhibit A

Curriculum Vitae of Professor Valtteri Niemi

CURRICULUM VITAE
13th May 2019

Name: Pentti **Valtteri NIEMI**
Male, Finnish citizen, born 11th September 1960
Postal address: Velusmaantie 61, 21140 Rymättylä, NAANTALI, Finland
Tel: +358 50 4837327
email: valtteri.niemi@helsinki.fi

Education and degrees:
Doctor of Philosophy, 25th May 1989, University of Turku, Department of Mathematics; Ph.D. thesis with highest grade (laudatur)
Master of Science, 29th January 1987, University of Turku, Department of Mathematics: highest grades

Current employment:
Professor in Computer Science, with specialty in Information Security, University of Helsinki, Finland, Department of Computer Science, from beginning of 2015. Deputy Head of the Department since 2016.

Most important career duties and titles:
Several positions in Academy of Finland projects, University of Turku and Vaasa Polytechnic Institute 1983-1992 (total 97 months); University of Turku, Associate Professor(acting) (*vs. apulaisprofessori)*, 1992-93 (12 months); University of Vaasa, Department of Mathematics and Statistics, Associate Professor in Mathematics (*ma. apulaisprofessori)*, 1993-97 (4 years); Nokia Research Center, Helsinki, various positions: starting as Senior Research Engineer and ending as Research Fellow and Distinguished Research Leader 1997-2008; Nokia Research Center, Lausanne, Switzerland, as Research Fellow 2008 and Nokia Fellow, 2008-2010; Nokia Research Center, Helsinki: as Distinguished Research Leader and Nokia Fellow, 2011-2012 (total 15 years); University of Turku, Department of Mathematics and Statistics, Professor in Mathematics (cryptography), 2012-2014 (part time still in 2015-2016)

Research visits:
Selected as a "High-end foreign expert" in China for 2014, located with Xidian University, Xi'an; spent in total two months there. Visited for total of one month also during each of the years 2016, 2017 and 2018.

Main awards:
Rolf Nevanlinna Ph.D. thesis award, 1990, for the best Finnish Ph.D. thesis in Mathematics; Nokia Quality Award, 2005, for the best Nokia research project (together with a team); Nokia Breakthrough Award 2008 for major impact technology transfer; Finnish Cyber Security Researcher of the Year 2016.

Recent research funding:
Academy of Finland project "Cloud Security Services", 2014-2016: 250 kiloEuros; sequel project "Cloud-assisted Security Services", funded by TEKES, 2016-2019: 450 kE; TEKES project TAKE-5, 2015-2018: 176 kE; Huawei Technologies bilateral research projects, 2016-2019: 830 kE; Intel donation grants, 2017-2018: 150 kE; EU H2020 project HELIOS, 2019-2021: 255 kE; Business Finland project 5GFORCE, 2019-2021: 550 kE.

Research leadership and supervision of doctoral and master level theses:
Contributions to several EU projects: Nokia-side leader in SHAMAN (Secure Heterogeneous Access for Mobile Applications and Networks) 2000-2002 and CYBERVOTE (An innovative cyber voting system for Internet terminals and mobile phones) 2000-2003; Contributions to several TEKES projects:

Nokia-side leader in TiViT SHOK program “Future Internet” 2011-2012; Nokia-side responsible for planning of TiViT SHOK program “Internet of Things” that started in 2012; Coordinator and Principal Investigator in Finnish Academy project “Cloud Security Services”, 2014-2016, PI in TEKES project “Cloud-assisted Security Services”, 2016-2018; PI and security task leader in TEKES project “TAKE-5” for 5G technologies, 2015-2018.
Approx. ten M.Sc. theses supervised, several more co-supervised from Nokia side; During Nokia time I had no official role in Ph.D. thesis supervision but some Ph.D. theses have been completed by members of my team(s) in Nokia, including Y. Zheng, 2007, D. Forsberg, 2010, K. Kostiainen 2012, J.-E. Ekberg 2013, all in TKK/Aalto.
One Ph.D. student officially supervised in University of Turku (Noora Nieminen, March 2017); Internet Laboratory responsible person for NRC Ph.D. program 2007-2008

Other scientific and academic duties:

Opponent/Committee member for Ph.D. dissertations:
Marko Hassinen, Univ. of Kuopio, Finland, 2006, Geir Koien, Univ of Aalborg, Denmark, 2008, Julien Freudiger, EPFL, Lausanne, Switzerland, 2010, Ravishankar Borgaonkar, TU Berlin, Germany, 2013, Matus Harvan, ETHZ, Zürich, Switzerland, 2013,Tuomas Kortelainen, Univ. of Oulu, Finland, 2014, Juha Partala, Univ. of Oulu, Finland, 2015, Yki Kortesniemi, Aalto University, Finland, 2015, Huihui Yang, Univ. of Agder, Norway, 2016, Sanna Suoranta, Aalto University, Finland, 2016, Mingjun Wang, Xidian University, China, 2017, Wenxiu Ding, Xidian University, China, 2017
External examiner for Ph.D. theses: six times
Several assessment duties for Adjunct Professorships (Docent)
In addition to job-related teaching, more than 10 additional courses lectured in academia and industry.
Recent Technical Program Committee memberships:
ETSI security workshop 2011-2013, FRUCT workshops 2011-2019, SSR 2014, 2016, 2018, IEEE CIT 2014, IEEE Trustcom 2015, ACM WiSec 2009, 2016, 2017, NordSec 2016, NSS 2017
Major role in organizing committees:
Eurocrypt 1998 (Financial Officer), Finnish Mathematical Days, 1995, Diderot Forum 2001, IEEE CIT 2014 (Panel Chair), IEEE Trustcom 2015 (co-General Chair), EAI MobiMedia 2016 (Workshop co-Chair/Panel Chair), NSS 2017 (co-General Chair), FRUCT 21 (General Chair), 2017, FRUCT 25 (General Chair), 2019.
Peer reviewer for many scientific journals and conferences

Other significant duties in industry/society:

Leader of several collaboration projects between Nokia and academic partners, Leader of more than 20 Nokia internal research projects and programs, Founding member of the Nokia Research Center Lausanne laboratory at EPFL campus 2008, Promoted to the highest technical expert rank of “Nokia Fellow” as fifth person in the company history in 2009, Chairman of the 3rd Generation Partnership Project (3GPP) security working group 2003-2009, (Vice chairman 2001-2003, Nokia main delegate in the above working group in 1999-2003), Nokia main delegate in ETSI GSM security working group (SMG10) 1997-1999, Board Member of Nokia Foundation 2010-2018 (vice chair 2017), Member of MATINE (Scientific Advisory Board for Defence) working group for ICT since 2013 (vice chair since 2016) and theme group for cybersecurity since 2016; Member of Finnish government working group for preparing voting over Internet, 2013-2015; Professor Union (*Professoriliitto,* in Finland): participation in various meetings as Univ. of Vaasa section representative 1994-97

Patents, invited lectures in conferences, publications:

34 patent families co-authored; Many essential patents for cellular standards; some used in litigation: e.g. two patents in Nokia vs Qualcomm; as a result Qualcomm acquired one of the patents; two other patents in Nokia vs. Apple; as a result Apple agreed to pay lump sum and royalties; in addition, 21 patent applications co-authored
22 invited talks in scientific conferences, seminars and workshops
18 invited talks in industrial conferences, seminars and workshops
80 original scientific articles in journals, refereed conferences and edited books
25 other scientific publications
4 published monographs, some translated to Chinese, Spanish and Russian
Total citations: 3340, h-index: 26 (Google Scholar)

Exhibit 19

11/8/2019 Huawei Ex Parte
(rebutting the Clarke Report)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket. Huawei seeks to clarify misconceptions regarding the relationship between its U.S. subsidiaries and the Chinese government.[1] Huawei previously submitted multiple expert law reports on Chinese laws, addressing misconceptions that these laws impose obligations on Huawei to assist the Chinese government in cyberespionage or other malicious activities.[2] But the

---

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs,* Draft Report and Order, Order, and Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC-CIRC1911-01, para. 47 (circulated Oct. 29, 2019) ("Draft Report and Order").

[2] Expert Report of Ariel Ye, Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, Ex. D (filed June 1, 2019); Expert Report of Jihong Chen and Jianwei Fang, Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, Ex. E (filed June 1, 2019); Supplemental Expert Report of Jihong Chen and Jianwei Fang, Reply Comments of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, Ex. B (filed Jul. 2, 2019); Expert Report of Dr. Hanhua Zhou, Ex Parte Written Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, Attachment A (filed May 5, 2019); Expert Opinion on

Chairman's proposal does not examine these reports. Instead, in designating Huawei as a covered company, the Chairman's proposal cites to a self-published "expert" report of Donald C. Clarke (the "Clarke Report") which aimed to rebut one of the Chinese law reports in the record.[3] Huawei now submits as **Attachment A** the rebuttal report of Mr. Jihong Chen, a partner and legal expert at the Zhong Lun Law Firm, which demonstrates that the Clarke Report provides an inaccurate analysis of Chinese law that is both misguided, and unsupported by evidence.

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, D.C. 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.

November 8, 2019

Article 17 of China's National Intelligence Law, Ex Parte Written Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89, Attachment A (filed Nov. 1, 2019).

[3] Draft Report and Order at n.130, 131.

Exhibit 19-A

Rebuttal Report of Jihong Chen to Professor Donald Clarke's Memorandum

Rebuttal to Prof. Donald Clarke's Memorandum "*The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law*"

Mr. Jihong CHEN
Partner
Zhong Lun Law Firm

November 8, 2019

I. INTRODUCTION

1. This Rebuttal issued by Mr. Jihong CHEN ("Zhong Lun" or "We") aims to rebut Prof. Donald Clarke's claims in his memorandum "*The Zhong Lun Declaration*[1] *on the Obligations of Huawei and Other Chinese Companies under Chinese Law*" dated 17 March 2019 (the "Donald Clarke Opinion").

2. This Rebuttal rebuts the claims in Part II (Summary) and Part IV (Analysis) of the Donald Clarke Opinion in sequence.

II. REBUTTAL

3. **Claim in the Donald Clarke Opinion (Para 3. a.):**

   "It is misleading because it misstates the key question of concern to the United States and other governments. That question is not what Chinese law says about the ability of the Chinese government to tell companies like Huawei what to do. The question is what the Chinese government can actually do, regardless of what the law might say. The Zhong Lun Declaration does not address the key issue of whether the Chinese government is meaningfully constrained by Chinese law."

4. **Rebuttal to Para 3. a. Claim[2]:**

   4.1 First, Prof. Clarke arbitrarily changed the "key question of concern to the United States and other governments" based on his own thinking. In fact, the key question of concern raised by the United States and other governments was directly derived from the enactment and enforcement of the *PRC Cyber Security Law*, the *PRC National Intelligence Law* and other relevant laws by the Chinese authorities (the "concerned laws"). Therefore, the real question of concern by the United States and other governments is with the obligations imposed on Huawei and the restrictions to the relevant law enforcement authorities' powers stipulated by the

[1] In this Rebuttal, the "Declaration" refers to the "Zhong Lun Declaration".

[2] In this Rebuttal, "Para n. Claim" stands for the claim in Para n. of the Donald Clarke Opinion.

concerned laws. Accordingly, a clear discussion of application of the above-mentioned laws, which is a discussion of legal issues, would help to resolve most of these concerns. In contrast, the question Prof. Clarke changed this to - "whether the Chinese government is meaningfully constrained by Chinese law" - is a different question that is principally a matter of fact.

4.2 Second, as explained in the Zhong Lun Declaration[3], the concerned laws provide regulations on the restrictions to the law enforcement authorities' power and the means of relief for individuals or organizations affected. Throughout the Donald Clarke Opinion, Prof. Clarke made arguments principally relying on his own conclusion that the Chinese government is not meaningfully constrained by Chinese laws no matter what the Chinese laws stipulate. Above all, Prof. Clarke's above-mentioned conclusion is just his personal view without any supporting evidence. In addition, the logic underlying Prof. Clarke's conclusion is obviously wrong. That is, if the Chinese government is not constrained by any law and there is no restriction to the Chinese government's power, laws *per se* would be meaningless in China and there would be no necessity for the Chinese government to enact laws. Further, in this hypothetical scenario, the United States and other governments would not need to worry about the promulgation and implementation of the concerned laws (at least there is no need to raise new worries of them), which is contrary to the current fact.

5. **Claim in the Donald Clarke Opinion (Para 3. b.):**

"It is misleading because even its legal analysis focuses entirely on statutory law passed by the National People's Congress and its Standing Committee. It does not look at lower-level regulations at all."

6. **Rebuttal to Para 3. b. Claim:**

First, according to Articles 96 and 97 of the *PRC Legislative Law*, if lower-level laws/regulations contravene higher-level laws/regulations, the relevant authorities shall amend or repeal the lower-level laws/regulations. Therefore, the underlying principle for the application of laws in China is that higher-level laws/regulations should prevail if lower-level laws/regulations contravene higher-level laws/regulations. Second, the Donald Clarke Opinion implies that the conclusion is misleading because the lower-level regulations which may affect the conclusion were not examined. However, the Donald Clarke Opinion does not provide any examples of such lower-level regulations "that were not examined. In fact, not every law must have corresponding lower-level regulations. Moreover, considering that those laws concerned were promulgated in recent years, it is normal that the corresponding lower-level regulations have not been enacted.

7. **Claim in the Donald Clarke Opinion (Para 3. c.):**

[3] *See*: Paragraphs 22-23, 43-47, 66-67, 81-83 of the Zhong Lun Declaration.

"It is inaccurate because in many places its analysis of the relevant laws attaches tremendous significance to a simple boilerplate statements such as that only 'relevant' organizations are subject to the law, or that the 'legitimate rights and interests' of citizens shall be respected. It interprets the latter statement as granting a powerful and wide-ranging right to regulated parties to reject Chinese government demands for cooperation. This reading of the law is unrealistic."

8. **Rebuttal to Para 3. c. Claim:**

8.1 Prof. Clarke's conclusion relies on his own assumption that the Chinese law enforcement authorities are not meaningfully constrained by Chinese laws no matter what the Chinese laws stipulate, or that the laws are interpreted arbitrarily. The Donald Clarke Opinion does not provide concrete evidence to support the claim that the Zhong Lun Declaration is inaccurate and that the reading of the law is unrealistic. *See* Paragraph 4.2 of this Rebuttal for details.

8.2 The claims in the Zhong Lun Declaration such as that only "relevant" organizations are subject to the law, or that the "legitimate rights and interests" of citizens shall be respected, are not simply boilerplate statements. For example, "the relevant organizations" which are subject to the check for the purpose of counterespionage work" usually means relevant organizations who own, hold or use electronic communication tools, devices, and other equipment or facilities, rather than any organizations or individuals unrelated thereto. Nor are telecommunications equipment manufacturers such as Huawei considered to be "relevant organizations". Moreover, if the government authorities misuse their powers to compel telecommunications equipment manufacturers to plant back doors, eavesdropping devices or spyware in the equipment they manufactured, such telecommunications equipment manufacturers may seek judicial relief under such laws as the *PRC Administrative Procedure Law*[4] to safeguard their "legitimate rights and interests". Accordingly, the claim in the Donald Clarke Opinion is unsupported.

9. **Claim in the Donald Clarke Opinion (Para 11.):**

"[T]he questions addressed by the Zhong Lun Declaration are limited to those of Chinese law. This is inadequate in three respects. First, the questions are only about statutory law passed by the National People's Congress and its Standing Committee. The Zhong Lun Declaration does not look at lower-level regulations at all. This is like attempting to understand U.S. securities law by looking only at congressional statutes and ignoring SEC rulemaking. Even if everything the Zhong Lun Declaration says about 'law' is accurate,

[4] For instance, Article 2 of the *PRC Administrative Procedure Law* provides that where citizens, legal persons or other organizations which consider that administrative acts of administrative organs or their personnel have infringed their legitimate rights and interests, they shall have the right to institute proceedings in people's courts according to this Law.

it is important to understand that it is talking about only a limited subset of mandatory rules and ignoring a vast universe of other mandatory rules."

10. **Rebuttal to Para 11. Claim:**

See Paragraph 6 of this Rebuttal.

11. **Claim in the Donald Clarke Opinion (Para 12.):**

"[I]t assumes - even asserts quite explicitly in several places - that if a citizen or organization believes its legal rights under law have been violated, it has an effective remedy available through the court system or via some other kind of administrative review. Particularly in the realm of state security, this belief is unjustified and in no way reflects Chinese reality. Many rights exist only on paper. In particular, rights that are vaguely and tautologically stated - for example, that a citizen's 'legitimate rights and interests' shall be protected - are meaningless for practical purposes, since among other things they leave unsaid what rights and interests shall count as legitimate."

12. **Rebuttal to Para 12. Claim:**

12.1 First, "legitimate rights and interests" is a concrete concept protected by the Chinese constitution. A citizen's "legitimate rights and interests" includes the lawful rights and interests of the citizen. The scope of "laws" that the "legitimate rights and interests" are based on includes the explicit provisions of laws and the basic principles of laws.[5] The implication of "legitimate" should mean that there is no express prohibition provided by laws.[6]

12.2 Second, in fact, the statistic report of the PRC Supreme People's Court shows that there have been over 2.3 million administrative judgements so far.[7]

12.3 Third, the Chinese government's official position supports our understanding. For example, at the PRC Ministry of Foreign Affairs Regular Press Conference on 18 February 2019, the spokesperson emphasized that "China's National Intelligence Law stipulates not only the obligations of organizations and individuals to lawfully support, assist and coordinate with the country's intelligence service, but also the obligations of the national intelligence service to carry out its work according to law, respect and protect human rights, and uphold the legal rights and interests of individuals and organizations. Meanwhile, there are many provisions in other laws to protect the legitimate rights and interests of

---

[5] With reference to Mr. Tao PENG (2010): *On the Legal Rights of the Plaintiff in Administrative Proceeding*, Journal of Political Science and Law, 27 (1), Page 87-92.

[6] *Ibid*.

[7] *See*: http://oldwenshu.court.gov.cn/List/List?sorttype=1&conditions=searchWord+3+AJLX++%E6%A1%88%E4%BB%B6%E7%B1%BB%E5%9E%8B:%E8%A1%8C%E6%94%BF%E6%A1%88%E4%BB%B6, last visited: 8 November 2019.

organizations and individuals, including data security and right to privacy. Those stipulations also apply to intelligence-related work."[8]

12.4 Accordingly, we could conclude that the administrative review/litigation legal system and relief system exist and run in China. Hence, the conclusion in the Zhong Lun Declaration which is based on the above laws and facts is more convincing than the conclusion in the Donald Clarke Opinion, which is primarily based on Prof. Clarke's own assumption.

13. **Claim in the Donald Clarke Opinion (Para 13.):**

"[E]ven if the Zhong Lun Declaration did look at the entire universe of mandatory rules in China, it would still fail to address the key question of concern to the United States and other governments. That question is not what Chinese law says about the ability of the Chinese government to tell companies like Huawei what to do. The question is what the Chinese government can actually do, regardless of what the law might say. The Zhong Lun Declaration does not address the key issue of whether the Chinese government is meaningfully constrained by Chinese law."

14. **Rebuttal to Para 13. Claim:**

See Paragraph 4 of this Rebuttal.

15. **Claim in the Donald Clarke Opinion (Para 14.):**

"[T]he Chinese political system is essentially Leninist, and recognizes no limits on government power, even as a matter of form. The Chinese Party/state is not meaningfully constrained by Chinese law. This is particularly so in matters deemed relevant to national security. The current incarceration of approximately one million Uyghurs in 'education and rehabilitation centers' is a prime example: it lacks the required statutory basis under China's own law, and yet proceeds unimpeded. The notion, advanced several times in the Declaration, that Chinese companies, if asked to do things by the Chinese security agencies for which those agencies had no legal mandate, could politely decline, and perhaps even bring lawsuits against the security agencies, is fanciful. The Zhong Lun Declaration cites no examples of anyone in China ever having done this successfully."

16. **Rebuttal to Para 14. Claim:**

First, all the opinions in the Zhong Lun Declaration are professional opinions from the legal perspective instead of the political perspective. Second, Prof. Clarke's conclusion relies on his own assumption that the Chinese law enforcement authorities are not meaningfully constrained by Chinese laws no matter what the Chinese laws stipulate or that the laws are interpreted arbitrarily. *See* Paragraph 4 of this Rebuttal for details.

---

[8] *See:* Foreign Ministry Spokesperson Shuang GENG's Regular Press Conference on 18 February 2019. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1638791.shtml, last visited: 8 November 2019.

17. **Claim in the Donald Clarke Opinion (Para 15.):**

"In an important sense, then, the entire Zhong Lun Declaration and the accompanying Clifford Chance Opinion are beside the point, because they fail to address the question that matters: the actual capacity of the Chinese government to do various things. Nevertheless, this memorandum will examine the legal arguments as well."

18. **Rebuttal to Para 15. Claim:**

See Paragraph 4 of this Rebuttal.

19. **Claim in the Donald Clarke Opinion (Para 17.):**

"This is in a sense true, but also misleading. The statutes do not purport to directly regulate companies organized outside of China. But they do regulate Huawei. If Huawei is obliged to do something under Chinese law, it is obliged to do so to the best of its ability. Thus, the fact that a U.S. subsidiary is not subject to Chinese law is irrelevant. The relevant fact is that it is subject to the control of its parent corporation. If Huawei exercises control over an overseas subsidiary (for example, a wholly-owned subsidiary), it is obligated to cause the subsidiary to act. Huawei chooses for business reasons to operate outside of China through subsidiaries with a separate corporate existence, as opposed to divisions or branches that have no separate corporate existence. It is undisputed that such divisions or branches, being part of Huawei itself, would enjoy no exemption from Huawei's obligations. It is inconceivable that Chinese law would allow organizations to manipulate their obligations simply by choosing to organize their overseas operations in one way as opposed to another."

20. **Rebuttal to Para 17. Claim:**

20.1 First, at least literally, the Donald Clarke Opinion agrees with the Zhong Lun Declaration on the conclusion that various statutes concerned regulate only Chinese entities and do not apply to Huawei's overseas subsidiaries.

20.2 Second, the claim in the Donald Clarke Opinion relies on Prof. Clarke's own assumption that the Chinese enforcement authorities would violate the laws and require Huawei to request its overseas subsidiaries to assist such work as the national intelligence work by planting back doors, eavesdropping equipment, or spyware in their equipment. In fact, such assumption lacks any evidence to support it.

20.3 Moreover, the Chinese government has repeatedly emphasized that the Chinese government has been asking Chinese companies to strictly abide by local laws and regulations when doing business overseas, and that China has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government

by installing back doors or by violating local laws.[9] *See* Paragraph 60 of this Rebuttal for details.

20.4 Furthermore, Huawei repeatedly declares that Huawei has not planted and will not plant back doors to assist the national intelligence work or engage in the espionage activities.[10]

21. **Claim in the Donald Clarke Opinion (Para 19. a.):**

"Chinese state security authorities generally operate beyond the law. They are rarely punished for exceeding their authority. The Declaration's assertion that they would be punished for exceeding their authority under the Counterespionage Law, for example, in the same way they would be punished for extorting a confession by torture does not inspire confidence, since it is conceded even by the Chinese authorities that a great deal of official torture still goes unpunished."

22. **Rebuttal to Para 19. a. Claim:**

First, this claim relies on Prof. Clarke's own assumption that the Chinese law enforcement authorities are not meaningfully constrained by Chinese laws no matter what the Chinese laws stipulate or that the laws are interpreted arbitrarily. *See* Paragraph 4 of this Rebuttal for details. Second, in fact, the statistic report of the PRC Supreme People's Court shows that there have been over 1.8 million administrative judgements so far.

23. **Claim in the Donald Clarke Opinion (Para 19. b.):**

"Similarly, the notion that affected parties could successfully sue the state security authorities in administrative proceedings is naive. Chinese courts will not defy state security authorities."

24. **Rebuttal to Para 19. b. Claim:**

This claim that "Chinese courts will not defy state security authorities" lacks grounds and is merely an assumption.

---

[9] *See:* (1) Foreign Ministry Spokesperson Shuang GENG's Regular Press Conference on 18 February 2019. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1638791.shtml, last visited: 8 November 2019. (2) Mr. Jiechi YANG, *Hope the United States (US) Side Will Work with the Chinese Side to Well Implement the Consensus of the Two Heads of State and Promote Bilateral Relations Based on Coordination, Cooperation and Stability.* https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1638953.shtml, last visited: 8 November 2019. (3) Foreign Ministry Spokesperson Kang LU's Regular Press Conference on 10 December 2018. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1620575.shtml, last visited: 8 November 2019. (4) The spokesperson of Embassy of China in Japan made similar comments in public on 07 December 2018. http://www.china-embassy.or.jp/chn/sgxxs/t1619923.htm, last visited: 8 November 2019.

[10] *See*: https://wallstreetcn.com/articles/3496863?from=groupmessage&isappinstalled=0, last visited: 28 March 2019; https://tech.sina.com.cn/it/2019-01-21/doc-ihqfskcn9148379.shtml, last visited: 28 March 2019.

25. **Claim in the Donald Clarke Opinion (Para 19. c.):**

"Nor is it remotely conceivable, as suggested in the Declaration, that individuals and organizations could successfully bring administrative review proceedings to challenge their designation as terroristic."

26. **Rebuttal to Para 19. c. Claim:**

This claim lacks grounds and is merely an assumption.

27. **Claim in the Donald Clarke Opinion (Para 19. d.):**

"The only way the Zhong Lun Declaration could substantiate its claim that its list of remedies is actually effective would be to provide examples of where they have worked in the past. It provides none."

28. **Rebuttal to Para 19. d. Claim:**

See Paragraphs 16 of this Rebuttal.

29. **Claim in the Donald Clarke Opinion (Para 21.):**

"'Espionage' is not clearly defined. The definition includes the catch-all term 'other activities of espionage'. The claim that law enforcement authorities must have explicit purposes and clear and specific goals is not supported in the text of the law. And as always, any claim that a legal standard is meaningful must be accompanied by an explanation of which institutions exist to make it meaningful. As noted above, the Declaration's repeated statements that affected parties may go to court to vindicate whatever rights the various statutes examined in the Zhong Lun Declaration may give them are fanciful and not reflective of actual Chinese reality."

30. **Rebuttal to Para 21. Claim:**

30.1 It should be noted that Article 38 of the *PRC Counterespionage Law* provides a detailed list to define acts of espionage which shall be prevented, stopped and punished. Besides, when interpreting Article 38 (5) of the *PRC Counterespionage Law*, "other activities" should be interpreted to the activities with the same nature as the activities listed before Article 38 (5) (i.e., Article 38 (1) - (4) of the *PRC Counterespionage Law*).[11]

30.2 Besides, as explained in the Zhong Lun Declaration, Article 13 of the *PRC Counterespionage Law* explicitly provides that its application shall be restricted to the needs for counterespionage work. It implies that law enforcement authorities should have explicit purposes and clear and specific goals.

30.3 Moreover, the claim in Donald Clarke Opinion that "the Declaration's repeated statements that affected parties may go to court to vindicate whatever rights the

[11] With Reference to Ms. Lanhua SHI (2012): *Application of the Miscellaneous Term under Legal Interpretation*, Journal of Hubei University of Police, 128 (5), Page 49-51.

various statutes examined in the Zhong Lun Declaration may give them are fanciful and not reflective of actual Chinese reality" lacks the evidence to support it.

31. **Claim in the Donald Clarke Opinion (Para 23.):**

"This is putting far more weight on an unimportant term - 'relevant' - than it can bear. Whether an organization is relevant or not is decided by the authorities. A company approached by the government with a request to cooperate is for that very reason 'relevant'. The Zhong Lun Declaration provides no examples of cases in which parties escaped the jurisdiction of a Chinese government agency on the grounds that the applicable statute covered only 'relevant' parties and that they were not relevant."

32. **Rebuttal to Para 23. Claim:**

See Paragraphs 16 of this Rebuttal.

33. **Claim in the Donald Clarke Opinion (Para 25.):**

"Even if the Zhong Lun Declaration were correct in its restrictive reading of 'checking' and its confidence that that reading would be upheld by Chinese courts against the wishes of the security services, it is mistaken in asserting that 'checking' is all that the security authorities are entitled to do. Article 22 of the law states that when security agencies are investigating espionage activities and collecting evidence, organizations and individuals may not refuse to provide it. It is not difficult to read into this language an obligation to implant spyware or engage in similar activities."

34. **Rebuttal to Para 25. Claim:**

The provision that "organizations and individuals may not refuse to provide it" in Article 22 of the *PRC Counterespionage Law* means that organizations and individuals may not refuse to provide relevant evidence of espionage that the organization already possesses. There is no word in Article 22 indicating that an individual or an organization has an obligation, as an intelligence agent, to collect the evidence or intelligence by planting spyware or engage in similar activities.

35. **Claim in the Donald Clarke Opinion (Para 27.):**

Misleading or wrong.

36. **Rebuttal to Para 27. Claim:**

See Paragraphs 22-28 of this Rebuttal.

37. **Claim in the Donald Clarke Opinion (Para 29.):**

Misleading or wrong.

38. **Rebuttal to Para 29. Claim:**

See Paragraphs 22-28 of this Rebuttal.

39. **Claim in the Donald Clarke Opinion (Para 31.):**

Misleading or wrong.

40. **Rebuttal to Para 31. Claim:**

See Paragraphs 19-20 of this Rebuttal.

41. **Claim in the Donald Clarke Opinion (Para 34.):**

"It does not. Like the *PRC Counterespionage Law*, the definition of terrorism includes a vague catch-all clause: 'other terrorist activities'."

42. **Rebuttal to Para 34. Claim:**

Paragraph 1 of Article 3 of the *PRC Anti-terrorism Law* provides a clear definition of the "terrorist activities". Therefore, "other terrorist activities" in Article 3 (5) of must be interpreted with reference to the definition of the "terrorist activities" in a specific case. Also *See* Paragraph 30.1 of this Rebuttal.

43. **Claim in the Donald Clarke Opinion (Para 36.):**

"First, the claim above does not address the question of the expansive term 'other terrorist activities'. It addresses only the question of whether the Chinese government would abuse its power through overly broad and unjustified classifications of terrorist groups and individuals. Second, it addresses that question by making the profoundly unrealistic claim that individuals and groups designated as terroristic can simply apply for administrative review and have their claims heard fairly by an institution with the will and capacity to restrain the state security authorities."

44. **Rebuttal to Para 36. Claim:**

See Paragraphs 42 and 12 of this Rebuttal.

45. **Claim in the Donald Clarke Opinion (Para 38.):**

"This claim appears to be accurate. I note, however, that the Zhong Lun Declaration states that Huawei is not obligated under the law 'where it acts as a manufacturer and seller of telecommunications equipment', implying that there may be times where it acts other than as a manufacturer and seller of telecommunications equipment and is therefore subject to the law.[12]"

46. **Rebuttal to Para 38. Claim:**

46.1 First, Prof. Clarke admitted that Huawei is not obligated under the law "where it acts as a manufacturer and seller of telecommunications equipment".

46.2 Although we could not exclude the possibility that Huawei may extend its business, where Huawei constitutes a telecommunications business operator and/or an Internet service provider, Huawei's obligations would be limited. Specifically, Huawei's obligations should be limited to those networks related to its service

[12] "The law" refers to the *PRC Cyber Security Law*.

operation as a telecommunications business operator and/or an Internet service provider, and should not extend to the telecommunications equipment manufactured and sold by it (as an equipment manufacturer and seller).

47. **Claim in the Donald Clarke Opinion (Para 40.):**

"The Zhong Lun Declaration does not cite a clear basis for its view that 'terrorist activities' must refer to a specific case and cannot refer to general measures designed to deal with what the state chooses to define as terrorism. Thus, its assertion that the scope of legal obligation is limited is valid only if one believes that there are limits on the Chinese government's ability to define what counts as 'terrorist activities' and what counts as 'assistance and support'. But there are no such limits."

48. **Rebuttal to Para 40. Claim:**

See Paragraph 42 of this Rebuttal.

49. **Claim in the Donald Clarke Opinion (Para 42.):**

Misleading or wrong.

50. **Rebuttal to Para 42. Claim:**

See Paragraphs 22-28 of this Rebuttal.

51. **Claim in the Donald Clarke Opinion (Para 44.):**

Misleading or wrong.

52. **Rebuttal to Para 44. Claim:**

See Paragraphs 19-20 of this Rebuttal.

53. **Claim in the Donald Clarke Opinion (Para 47.):**

"The premise is correct, but the conclusion does not follow. The Chinese government is not limited by law. There is no institution in China that could determine that the state security agencies had overstepped the bounds of the Cybersecurity Law and provide an effective remedy."

54. **Rebuttal to Para 47. Claim:**

It seems that the Donald Clarke Opinion agrees with the Zhong Lun Declaration at least from the legal perspective on the conclusion that the purpose of the law is to protect China's cyber security, not to threaten the cyber security of any other country. Thus, the authorities could not use the law for any purpose beyond this scope. The Donald Clarke Opinion believes that "the conclusion does not follow" only because Prof. Clarke made his conclusion based on his own assumption that the Chinese government is not meaningfully constrained by Chinese laws no matter what the Chinese laws stipulate. *See* Paragraph 4 of this Rebuttal for details.

55. **Claim in the Donald Clarke Opinion (Para 49. a.):**

"'Network' is not clearly defined in the Cybersecurity Law, and therefore 'network operator' is not clearly defined. There is little question that the term extends beyond ordinary internet service providers. Chinese banks have argued in overseas legal proceedings that it covers them as well, since they store data in internal networks. To the extent Huawei's internal networks are less accessible to the public that those of banks, it is plausible to argue that it is not a 'network operator'. Nevertheless, the question is not clear. There is sufficient ambiguity that if the state security authorities wished to deem Huawei a network operator on the basis of its internal networks, it is hard to see how they could be prevented from doing so."

56. **Rebuttal to Para 49. a. Claim:**

Firstly, according to Article 9[13] of the *PRC Cyber Security Law*, " network operators" are limited to those operators who carrying out business operation and service activities rather than operating their internal network. Secondly, the Cyber Security Legal Research Centre of No. 3 Research Institute of the PRC Ministry of Public Security[14] has summarized almost all publicly known law enforcement actions under the *PRC Cyber Security Law* between June and August 2017. According to this article, all these enforcement actions are against network operators that carry out business operations and service activities to the public.

57. **Claim in the Donald Clarke Opinion (Para 49. b.):**

"Note, however, the statement's qualification: '[w]hen Huawei, as a manufacturer of telecommunications equipment, engages in R&D and production and sale of telecommunications equipment……' This of course implies that Huawei could be considered a network operator for other reasons. If so, it would be subject to the law. Consequently, the fact that it is not a network operator for one set of reasons is not particularly relevant."

58. **Rebuttal to Para 49. b. Claim:**

See Paragraph 46.2 of this Rebuttal.

59. **Claim in the Donald Clarke Opinion (Para 51.):**

"The Zhong Lun Declaration provides no support for its assertion that the broad term 'technical support and assistance' does not include the specific actions it mentions. It is simply declaring this to be true. Without more, the bare assertion is not credible. In the

[13] Article 9 under the *PRC Cyber Security Law* provides that "[w]hen carrying out business operation and service activities, network operators shall abide by laws and administrative regulations, show respect for social moralities, follow business ethics, and act in good faith. They shall also fulfill the obligation of cybersecurity protection, accept governmental and public supervision, and undertake social responsibilities."

[14] Cyber Security Legal Research Centre of No. 3 Research Institute of the PRC Ministry of Public Security, *Analysis on Certain Issues under Administrative Enforcement of the PRC Cyber Security Law*, published on 29 September 2017, available at Wolters Kluwer.

Chinese legal system, vagueness and ambiguity are interpreted in favor of the authorities, not against them.

60. **Rebuttal to Para 51. Claim:**

In addition to the literal interpretation of the law, the Chinese government has taken a consistent position on the issue whether the Chinese companies are required by Chinese laws to provide assistance to the national intelligence work through installing mandatory back doors or violating local laws of other countries. For example:

60.1 On March 15, 2019, Chinese Premier Li Keqiang[15] met the press after the conclusion of the second session of the 13th National People's Congress (NPC) at the Great Hall of the People in Beijing and said publicly that "[t]he Chinese government did not and will not ask Chinese companies to spy on other countries, such kind of action is not consistent with the Chinese law and is not how China behaves."

60.2 At 18 February 2019 PRC Ministry of Foreign Affairs Regular Press Conference, the spokesperson emphasized that "the Chinese government has been asking Chinese companies to strictly abide by local laws and regulations when doing business overseas; this position will not change…China has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government by installing 'back doors' or by violating local laws."[16]

60.3 At a press meeting of the 55th Munich Security Conference on 16 February 2019, Mr. Yang Jiechi, Member of the Political Bureau of the CPC Central Committee and Director of the Office of the Central Commission for Foreign Affairs of China, pointed out that "the Chinese government always requires Chinese companies to abide by international rules and laws and regulations of the country where they operate. Over a long period, Huawei Technologies Co., Ltd. has made positive contributions to the development of communication technologies in countries including in Europe, and strictly abided by international rules and local laws and regulations in this process."[17]

---

[15] *See*: *Chinese government did not and will not ask companies to engage in spying: premier*, http://www.xinhuanet.com/english/2019-03/15/c_137897399.htm, last visited: 8 November 2019.

[16] *See*: Foreign Ministry Spokesperson Shuang GENG's Regular Press Conference on 18 February 2019. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1638791.shtml, last visited: 8 November 2019.

[17] *See*: Mr. Jiechi YANG, *Hope the United States (US) Side Will Work with the Chinese Side to Well Implement the Consensus of the Two Heads of State and Promote Bilateral Relations Based on Coordination, Cooperation and Stability.* https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1638953.shtml, last visited: 8 November 2019.

60.4 At 10 December 2018 PRC Ministry of Foreign Affairs Regular Press Conference on, the spokesperson emphasized that Chinese laws and regulations never give any institution the mandate to force companies to build "mandatory back doors".[18]

61. **Claim in the Donald Clarke Opinion (Para 53.):**

Misleading or wrong.

62. **Rebuttal to Para 53. Claim:**

See Paragraphs 22-28 of this Rebuttal.

63. **Claim in the Donald Clarke Opinion (Para 55.):**

Misleading or wrong.

64. **Rebuttal to Para 55. Claim:**

See Paragraphs 22-28 of this Rebuttal.

65. **Claim in the Donald Clarke Opinion (Para 57.):**

Misleading or wrong.

66. **Rebuttal to Para 57. Claim:**

See Paragraphs 19-20 of this Rebuttal.

67. **Claim in the Donald Clarke Opinion (Para 60.):**

"This is one of the most preposterous claims of the Declaration. Language in Chinese statutes about protecting 'legitimate rights and interests' is essentially meaningless boilerplate. Among other things, it leaves unanswered the question of which rights and interests count as legitimate. It is inconceivable that a Great Wall of resistance to Chinese state authority could be built upon such a flimsy linguistic foundation. No Chinese authority to my knowledge has ever acknowledged that the interest of Chinese companies and individuals in doing business and making money trumps the state's interest in national security. Furthermore, it is impossible to believe that the Chinese state would consider the prospect of punishment under foreign law as a valid reason for refusing an otherwise valid demand to cooperate. The United States recognizes no such general exemption; still less does China. That would be to allow foreign governments the power to constrain the regulatory authority of the Chinese government over Chinese parties in China, and that would clearly be unacceptable."

68. **Rebuttal to Para 60. Claim:**

68.1 First, the implication of the "legitimate rights and interests" has been explained in Paragraph 12 of this Rebuttal. *See* Paragraph 12 of this Rebuttal for details.

---

[18] *See*: Foreign Ministry Spokesperson Kang LU's Regular Press Conference on 10 December 2018. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1620575.shtml, last visited: 8 November 2019.

68.2 Second, state security should be protected in accordance with the law. As explained above, the Chinese law does not authorize the state authorities to require the telecommunications equipment manufacturers to plant back doors, eavesdropping equipment, or spyware in their equipment. Therefore, if the telecommunications equipment manufacturers were requested to plant back doors, eavesdropping equipment, or spyware in their equipment in the guise of assisting the state security protection, such requests would be unlawful given it exceeds the scope of legal authorization and would infringe upon the "legitimate rights and interests" of the telecommunications equipment manufacturers. Under this circumstance, the telecommunications equipment manufacturers could refuse the unlawful requests.

68.3 Third, as explained in Paragraph 60 of this Rebuttal, the Chinese government is taking a consistent stand on the issue whether the Chinese companies are required by Chinese laws to provide assistance to the national intelligence work through installing mandatory back doors or violating local laws of other countries. The official stand demonstrates that individuals and organizations shall have the right to refuse to obey requests for cooperation made by national intelligence agencies, particularly if the cooperation relationship would result in violation of local applicable laws of another country. *See* Paragraph 60 of this Rebuttal for details.

69. **Claim in the Donald Clarke Opinion (Para 64.):**

"This is another preposterous claim. 'In accordance with law' is another example of essentially meaningless boilerplate. It is incorrect to suggest that every type of request for cooperation must have a specific basis in law. There is no law explicitly authorizing the state security authorities to do anything specific when they request cooperation, and yet nobody supposes that they are therefore crippled. Chinese laws are highly general and simply do not get into specifics like this. It might equally be observed that there is no law specifically authorizing the state intelligence agencies to make cooperation requests on a Tuesday, but nobody doubts they have the power to do so."

70. **Rebuttal to Para 64. Claim:**

70.1 "In accordance with law" is not meaningless boilerplate. The requirement that requests or provisions of support, assistance and cooperation should be "in accordance with law" has the following two implications:

First, under the Chinese legal system, a requirement must be codified into law before becoming a legal obligation for individuals and organizations. However, there is no such law in China whatsoever authorizing national intelligence agencies to require telecommunications equipment manufacturers to plant back doors, eavesdropping equipment, or spyware, nor is there any Chinese law that imposes a legal obligation on individuals and organizations to do so.

Second, the reference to "in accordance with law" means that the state authorities are not empowered to request individuals and organizations to carry out any

unlawful activity, and the individuals and organizations are not obliged to comply with any request to carry out any unlawful activity. Requests for planting back doors, eavesdropping equipment, or spyware in the telecommunications equipment would be considered as unlawful requests as it may result in potential breaches of some applicable laws and regulations of China. This is another reason why Huawei is not obliged to comply with any request to plant back doors, eavesdropping equipment, or spyware in their telecommunications equipment. For example, requests for planting back doors, eavesdropping equipment, or spyware in the telecommunications equipment would contravene Article 27 of the *PRC Cyber Security Law*. Article 27 of the *PRC Cyber Security Law* provides that, any individual or organization shall neither engage in activities endangering cyber security, including illegally invading others' networks, interfering with the normal functions of others' networks and stealing cyber data, nor provide programs or tools specifically used for activities endangering cyber security, such as network intrusions, interference with the normal functions and protective measures of the network, and theft of cyber data; if such individual or organization knows that a person engages in activities jeopardizing cyber security, it shall not provide technical support, advertising promotion, payment and settlement services or other types of assistance to such person or organization.

70.2 Besides, as explained in Paragraph 60 of this Rebuttal, the Chinese government is taking a consistent stand on the issue of whether the Chinese companies are required by Chinese laws to provide assistance to the national intelligence work by installing mandatory back doors or violating local laws of other countries. That is, the Chinese government has been asking Chinese companies to strictly abide by local laws and regulations when doing business overseas. China has not asked and will not ask companies or individuals to collect or provide data, information and intelligence stored within other countries' territories for the Chinese government by installing 'back doors' or by violating local laws. *See* Paragraph 60 of this Rebuttal for details.

71. **Claim in the Donald Clarke Opinion (Para 66.):**

"Even if this claim were true - which it is not - the Constitution is not part of the enforceable legal system of China. Chinese courts do not have the power to invalidate government actions on constitutional grounds, even in the unlikely event that a particular judge should be inclined to do so. Thus, constitutional arguments are simply irrelevant here. In any case, the claim is not true. The section of the Constitution cited in the Zhong Lun Declaration (Article 40) is about protecting the privacy of Chinese citizens. The concern of the U.S. and other governments is about Huawei being required to infringe on the privacy of non-Chinese persons and organizations. Huawei could do that without infringing on the privacy of Chinese citizens."

72. **Rebuttal to Para 66. Claim:**

72.1 The *Constitution of the PRC* is the fundamental law of the Chinese legal system. The rights and interests of citizens and legal persons stipulated in the *Constitution of the PRC* are intended to be embodied in specific law branches, like the *General Rules of the Civil Law of the PRC* and the *PRC Tort Law*. Therefore, if the constitutional rights and interests of the citizens and legal persons are infringed, such citizens and legal persons have rights to file lawsuits with the court according to the specific provisions of the specific laws. For example, Article 110 of the *General Rules of the Civil Law of the PRC* stipulates that natural persons have the right to privacy, and Article 111 of the *General Rules of the Civil Law of the PRC* stipulates that any organization or individual shall legally obtain the personal information of others when necessary and ensure the safety of such personal information, and shall not illegally collect, use, process or transmit the personal information of others, or illegally buy or sell, provide or make public the personal information of others. Also, Article 2 of the *PRC Tort Law* stipulates that the right to privacy shall not be infringed. Therefore, if an individual's right under Article 40 of the *Constitution of the PRC* is infringed, he or she may bring a lawsuit to the relevant courts in accordance with the relevant provisions of the *General Rules of the Civil Law of the PRC* and the *PRC Tort Law*. Under this circumstance, if the infringer is the state authorities, such state authorities may be sued under the *PRC Administrative Review Law* and the *PRC Administrative Procedure Law*.

72.2 In addition, according to Article 32 of the *Constitution of the PRC*, China protects the lawful rights and interests of foreign citizens in Chinese territory. Therefore, the privacy of the foreign citizens in China could also be protected. Regarding the foreign citizens outside China, their "legitimate rights and interests" would also be respected - as the Chinese government has reiterated. For instance, at the PRC Ministry of Foreign Affairs Regular Press Conference on 18 February 2019, the spokesperson emphasized that "China's National Intelligence Law stipulates not only the obligations of organizations and individuals to lawfully support, assist and coordinate with the country's intelligence service, but also the obligations of the national intelligence service to carry out its work according to law, respect and protect human rights, and uphold the legal rights and interests of individuals and organizations. Meanwhile, there are many provisions in other laws to protect the legitimate rights and interests of organizations and individuals, including data security and right to privacy. Those stipulations also apply to intelligence-related work".[19]

73. **Claim in the Donald Clarke Opinion (Para 68.):**

Misleading or wrong.

[19] *See:* Foreign Ministry Spokesperson Shuang GENG's Regular Press Conference on 18 February 2019. https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/t1638791.shtml, last visited: 8 November 2019.

74. **Rebuttal to Para 68. Claim:**

See Paragraphs 22-28 of this Rebuttal.

75. **Claim in the Donald Clarke Opinion (Para 70.):**

Misleading or wrong.

76. **Rebuttal to Para 70. Claim:**

See Paragraphs 19-20 of this Rebuttal.

I declare that the foregoing is true and correct under penalty of perjury of the laws of the United States of America.

Executed on November 8, 2019

Beijing, P. R. China

Chen Jihong

Exhibit 20

11/12/2019 Huawei Ex Parte
(providing positive international assessments of Huawei's equipment and security)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket. Huawei responds to the assertion that "several of the United States' closest allies have concluded that the risk posed by Huawei equipment and systems is too great to bear."[1] Huawei disagrees that "similar assessments by other countries"[2] support the Chairman's proposal to designate Huawei as a covered company. To the contrary, U.S. allies have used and plan to continue to use Huawei equipment in their networks, including in facilitation of 5G deployment.

---

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Draft Report and Order, Order, and Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC-CIRC1911-01, para. 50 (circulated Oct. 29, 2019) ("Draft Report and Order").

[2] *Id.*

Huawei has previously submitted evidence that many other countries have not found its equipment to pose a risk.[3] In fact, much of Europe, Africa, the Middle East, and the Americas plan to deploy 5G networks with at least some Huawei equipment.[4] For example, the U.K., a member of the Five-Eyes, has recently indicated that it plans to allow Huawei equipment in its 5G network.[5] And Germany recently finalized rules for 5G deployment that do not exclude Huawei from its networks, in an effort to create a "level playing field" for vendors.[6] Chancellor Angela Merkel reaffirmed Germany's position last week, acknowledging Huawei's active participation in 2G and 3G expansion, and noting that Germany will not issue any guidelines for individual providers.[7] German operators had previously cautioned that banning Huawei would "add years of delays and

---

[3] *Ex Parte* Written Submission of Huawei Technologies Co., Ltd. and Huawei Technologies USA, Inc., WC Docket No. 18-89 (filed Mar. 12, 2019).

[4] Amy Cheng and Emily Feng, "China's Tech Giant Huawei Spans Much of the Globe Despite U.S. Efforts to Ban It," NATIONAL PUBLIC RADIO (Oct. 24, 2019), *available at* https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it ("Much of Europe, Africa, the Middle East and the Americas will continue to set up 5G using at least some Huawei equipment. Some countries have directly pushed back against American pressure, declaring it their sovereign choice.").

[5] Richard Kerbaj and Tim Shipman, "Johnson Set to Grant Huawei Access to UK's 5G Network and Open Rift with Trump," THE TIMES (Oct. 26, 2019), *available at* https://www.thetimes.co.uk/edition/news/johnson-set-to-grant-huawei-access-to-uks-5g-network-and-open-rift-with-trump-fccqvcrsj?wgu=270525_54264_15725151998543_ee1cb6095c.

[6] "Germany Will Not Bar Huawei from its 5G Networks," BBC (Oct. 16, 2019), *available at* https://www.bbc.com/news/technology-50068415.

[7] "Merkel trotz Pompeo-Warnung gegen Ausschluss von Huawei bei 5G-Ausbau [Merkel, Despite Pompeo Warning, Against Exclusion of Huawei at 5G Expansion]," HANDELSBLATT (Nov. 8, 2019), *available in German at* https://www.handelsblatt.com/dpa/wirtschaft-handel-und-finanzen-merkel-trotz-pompeo-warnung-gegen-ausschluss-von-huawei-bei-5g-ausbau/25206660.html.

billions of dollars in costs to launching 5G networks."[8] Indeed, some countries have already begun to reap the economic and other benefits of Huawei's innovative and advanced technology: Greece has partnered with Huawei for two 5G pilot networks;[9] and Portugal is on track to establish its first 5G mobile city through a partnership with Huawei.[10]

The Draft Report and Order references the European Union's risk assessment on 5G security (the "Risk Report") as further evidence of purported international support for its proposed rule.[11] But the proposed rule is inconsistent with the purpose of the Risk Report, which was to "define one common position on the 5G mobile network without excluding any company, from any country."[12] As Portugal's Foreign Affairs minister recently remarked, the 5G risk assessment "is not a question related to company A, B, C or D," but to the "need to take the necessary measures to guarantee an infrastructure that complies with all the security requirements from the state's point of view and for the citizens' personal data."[13]

---

[8] *Id.*; *see also* Douglas Busvine and Andreas Rinke, "New German Rules Leave 5G Telecoms Door Open to Huawei," REUTERS (Oct. 14, 2019), *available at* https://www.reuters.com/article/us-germany-telecoms-5g/new-german-rules-leave-5g-telecoms-door-open-to-huawei-idUSKBN1WT110.

[9] Bojan Stojkovski, "As US, China Fight Trade War, Greece Opens Up to Huawei's 5G Ambitions," ZDNET (Aug. 19, 2019), *available at* https://www.zdnet.com/article/as-us-china-fight-trade-war-greece-opens-up-to-huaweis-5g-ambitions/.

[10] Leian Kae Naduma, "Huawei, China, Portugal Builds 5G City, What Comes in it?," BUSINESS TIMES (Oct. 25, 2019), *available at* https://en.businesstimes.cn/articles/120818/20191025/huawei-china-portugal-builds-5g-city-what-comes-with-it.htm.

[11] *Supra* n.1.

[12] "Portugal Willing to Allow Huawei to Build 5G Network Infrastructure," TECHQOON (Apr. 30, 2019), *available at* https://techqoon.net/2019/04/30/portugal-willing-to-allow-huawei-to-build-5g-network-infrastructure/.

[13] *Id.*

Huawei notes that the Risk Report was published by European Union member states and based upon national risk assessments that those member states undertook earlier this year. Importantly, none of these member states have plans to exclude Huawei—and many have stated publicly that they *will not* exclude Huawei. Instead, it appears that much of the international community recognizes the importance of a holistic cybersecurity approach that is based on a true risk assessment methodology rather than applying a blanket, country-of-origin ban. For example, in the wake of recent news that Huawei will work with Vodafone and Deutsche Telekom to build Hungary's 5G network, Hungarian Foreign Minister Peter Szijjarto remarked that Hungary rejects discriminating against companies based on nationality.[14] France has long indicated that it does not intend to exclude Huawei, instead relying on existing safeguards for cybersecurity.[15] Similarly, the Dutch government, which has also declined to exclude Huawei from its 5G infrastructure, announced earlier this year that it is addressing potential security vulnerabilities and cyberespionage by requiring companies to thoroughly vet their equipment suppliers against "extra high standards."[16] And outside of the European Union, Norway has done the same in opting against

---

[14] Zoltan Simon, "Viktor Orban Defies Trump to Back Huawei Role in Hungary's 5G Networks," BLOOMBERG (Jul. 1, 2019), *available at* https://www.bloomberg.com/news/articles/2019-11-05/orban-defies-trump-to-back-huawei-role-in-hungary-s-5g-networks.

[15] Jean-Baptiste Vey, "Macron Says it is not France's Aim to Block Huawei," REUTERS (May 16, 2019), *available at* https://www.reuters.com/article/us-huawei-security-france/macron-says-it-is-not-frances-aim-to-block-huawei-idUSKCN1SM0UU; Mathieu Rosemain, Gwenaelle Barzic and Elizabeth Pineau, "French Senate Rejects Tougher Telecoms Controls Despite U.S. Huawei Warning," REUTERS (Feb. 6, 2019), *available at* https://www.reuters.com/article/us-huawei-europe-france/french-senate-rejects-tougher-telecoms-controls-despite-u-s-huawei-warning-idUSKCN1PV2B8.

[16] Toby Sterling, "No Huawei Ban in Dutch 5G Rollout: Government," REUTERS (Jul. 1, 2019), *available at* https://www.reuters.com/article/us-netherlands-telecoms/no-huawei-ban-in-dutch-5g-rollout-government-idUSKCN1TW2V8.

a ban: its cabinet minister recently stated that the Norwegian government "has a good dialogue with the companies on security, and then it is up to the companies themselves to choose suppliers."[17]

Huawei urges the Commission to acknowledge the complex global nature of the communications supply chain, and to recognize—as many of its European Union allies have—that banning a supplier based on its country of origin is not an appropriate or effective solution for addressing security threats to the integrity of communication networks or the communications supply chain. Moreover, as evidenced by the warnings of German and U.S. carriers alike, such a ban would come at a great cost. Huawei encourages the Commission to consider the contents of the Risk Report in their totality, rather than cite selected passages out of context—including the recognition that a lack of vendor diversity increases exposure to risk, that 5G is already inherently more secure than 4G, and that the goal should be the "identification of a toolbox of appropriate, effective, and proportionate possible risk management measures to mitigate cybersecurity risks."[18]

---

[17] Victoria Klesty, "Norway Will not Ban Huawei from 5G Mobile Network: Minister," REUTERS (Jul. 1, 2019), *available at* https://www.reuters.com/article/us-norway-huawei-tech/norway-will-not-ban-huawei-from-5g-mobile-network-minister-idUSKBN1WB15G.

[18] European Union, EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks at 7, 23-24, 30, 33 (2019)

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, D.C. 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.

November 12, 2019

Exhibit 21

11/14/2019 Huawei Ex Parte
(addressing the FCC's alleged authority under the Communications Assistance for Law Enforcement Act)

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 the Federal Communications Commission ("FCC" or "Commission") to supplement the record in the above-captioned docket. In particular, Huawei responds to the Commission's claim that its *Draft Report and Order*'s prohibition against expenditure of Universal Service Fund ("USF") support on equipment or services produced or provided by certain companies that allegedly pose national security threats to the integrity of communications networks or the communications supply chain "implements section 105" of the Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1004.[1] Huawei also sets forth several additional reasons that the Commission's actions in the *Draft Report and Order* are unlawful.

---

[1] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Draft Report and Order, Order, and Further Notice of Proposed Rulemaking, WC Docket No. 18-89, FCC-CIRC1911-01, paras. 35-36 (circulated Oct. 29, 2019) ("*Draft Report and Order*") (*citing Communications Assistance for Law Enforcement Act and Broadband Access and Services*, Report and Order and Further Notice of Proposed Rulemaking, 20 FCC Rcd. 14989, 14992-97, paras. 9-14 (2005) ("*2005 CALEA Order*"), *pet. for rev. denied, American Council on Educ. v. FCC*, 451 F.3d 226 (D.C. Cir. 2006)).

I. The Commission May Not Invoke CALEA as Authority for the Rule

The Commission's reliance on section 105 of CALEA is misplaced for numerous reasons. *First*, the draft rule is not a logical outgrowth of the Notice of Proposed Rulemaking ("NPRM").[2] *Second*, the interpretation of the statute, including the term "switching premises," in the *Draft Report and Order* departs from CALEA's plain text; ignores statutory structure, purpose, and legislative history; is unauthorized by CALEA's rulemaking authority; and otherwise is unreasonable and lacks any meaningful limiting principle. *Third*, this overly expansive interpretation of "switching premises" contradicts the specific terms of CALEA and unreasonably and impermissibly expands its reach. *Finally*, there is no nexus between CALEA, which applies generally to all telecommunications carriers, and eligibility for USF support.

A. The Draft Rule Is Not a Logical Outgrowth of the Proposed Rule

As an initial matter, the Commission cannot rely on CALEA as a source of authority for its rule because it never proposed to rely on CALEA in its NPRM. Thus, a rule based on CALEA would not be a logical outgrowth of the rule proposed in the NPRM. A rule is a logical outgrowth of its notice only if parties "should have anticipated that the change [in approach from the notice] was possible, and thus reasonably should have filed their comments on the subject during the notice-and-comment period." *CSX Transp., Inc. v. Surface Transp. Bd.*, 584 F.3d 1076, 1080 (D.C. Cir. 2009) (citation and internal quotation marks omitted). But a rule flunks that test if "interested parties would have had to divine [the agency's] unspoken thoughts." *Id.* (citation and internal quotation marks omitted).

---

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

The Commission cannot meet that test here with respect to its invocation of CALEA. In the *Draft Report and Order*, the Commission cites two provisions of CALEA, 47 U.S.C. §§ 229 and 1004. But the Commission cited § 229 *nowhere* in the NPRM and cited § 1004 only in a footnote with no explanation or context whatsoever. NPRM, ¶ 36 n.64. Moreover, the Commission never cited *any* provision of CALEA as authority for the rule. NPRM, Appendix A (listing other purported sources of authority for the proposed rule). If the Commission wanted to rely on CALEA, it had to provide notice and an opportunity for comment. Had it done so, it would have learned at least the reasons set forth in detail below why such an interpretation exceeds the terms of the statute and otherwise makes no sense. But the Commission failed to put anyone on notice that it might attempt to base its USF rule on CALEA. Huawei and other commenters thus were deprived of the opportunity to develop and submit expert testimony on the issue—such as evidence to affirmatively contradict the FCC's unsupported speculation about eligible telecommunications carriers' using USF funds to facilitate unauthorized surveillance (*infra* pp. 14-15). A rule purportedly based on CALEA cannot be considered a logical outgrowth of the NPRM and is defective for that reason alone, quite apart from its substantive invalidity.

B. The FCC's Proposed Interpretation of CALEA Departs from the Statute's Plain Text, Ignores Statutory Structure, Purpose, and Legislative History, and Is Otherwise Patently Unreasonable

Section 105 of CALEA provides as follows:

> A telecommunications carrier shall ensure that any interception of communications or access to call-identifying information *effected within its switching premises* can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission.[3]

---

[3] 47 U.S.C. § 1004 (emphasis added).

In the *Draft Report and Order*, the Commission interprets the term "switching premises" "as including all points in a carrier's network where an interception might be activated." *Draft Report and Order*, ¶ 35. This interpretation is patently unreasonable and ignores all ordinary tools of statutory construction.

1. CALEA's plain text cannot sustain the draft rule

The cardinal rule of statutory construction is "that a legislature says in a statute what it means and means in a statute what it says there." *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992). "[E]very clause and word of a statute" must be given effect, and, "if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." *Duncan v. Walker*, 533 U.S. 167, 174 (2001) (citations omitted). Consequently, when section 105 states that it applies to communications interceptions "effected within [a carrier's] switching premises," 47 U.S.C. § 1004, that is exactly what the statute means: the statute covers communications interceptions only when they are effected within a carrier's switching premises. There is no ambiguity to sort out.

The Commission acknowledges that "the statutory language uses the term 'switching premises.'" *Draft Report and Order*, ¶ 35. The Commission nonetheless claims that it can interpret section 105 to apply to "*all points* in a carrier's network where an interception might be activated"—regardless, apparently, of whether any particular point is actually within the carrier's switching premises. *Id.* (emphasis added). Arrogating to itself the power to legislate, the Commission reads "switching premises" right out of the statute. The Commission has no authority to do so, especially when, as explained below, Congress' "switching premises" language is not a mere technicality but is a central component of CALEA's scheme.

2. CALEA's structure, purpose, and context likewise forbid the Commission to interpret CALEA to authorize the draft rule

CALEA's structure and purpose make clear that the statute applies only to interception of communications by law enforcement or via tools created by carriers to permit interception of communications by law enforcement—*not* to any and all attempts by other actors (such as foreign governments) to intercept communications. Yet the *Draft Report and Order* does not so much as acknowledge CALEA's focus—which is evident in the statute's very name. In addition, the Commission cannot reconcile CALEA's applicability to all carriers with a regulation limited to the USF context, which is governed by different statutory provisions. And even if it could, CALEA would prohibit precisely the type of rule the Commission has drafted.

a. CALEA's several provisions make clear that the statute enables *the government* to intercept communications, and that the restrictions on interception are, consequently, targeted at *the government* or the capabilities the statute requires carriers to implement in order to enable *the government* to effect interception. The draft rule, however, is entirely unrelated to enabling the government to effect communications interceptions or preventing the abuse of those capabilities.

To begin, CALEA requires telecommunications carriers to make tools available to "enabl[e] *the government*" to intercept communications "pursuant to a court order or other lawful authorization." 47 U.S.C. § 1002(a) (emphasis added) (listing the four interception capabilities required by the government); *see also id.* § 1001(5) ("The term 'government' means the government of the United States and any agency or instrumentality thereof, the District of Columbia, any commonwealth, territory, or possession of the United States, and any State or political subdivision thereof *authorized by law to conduct electronic surveillance*." (emphasis added)). The subject of the statute is authorized interception of communications by the government, and "authorization"

under CALEA plainly refers to authorization by law or a court for the government to intercept communications.

This context also shows why § 1004 does not reach beyond a carrier's "switching premises" and why it requires "the affirmative intervention of an individual officer or employee of the carrier." A carrier is required by law to be capable of "delivering intercepted communications . . . *to the government*, pursuant to a court order or other lawful information, . . . to a location *other than the premises of the carrier*." 47 U.S.C. § 1002(a)(3) (emphases added). The carrier must have the capability of intercepting communications *on its premises* and sending them to the government; consequently, the carrier must guard against the improper use of those statutorily required capabilities. And by requiring the affirmative participation of a carrier employee, Congress placed the controls in the carrier's hands to protect against law enforcement abuse. But the statute does not impose any requirement of interception capabilities on a carrier beyond its switching premises, and, correspondingly, does not impose any requirements for preventing interception *beyond* the carrier's switching premises. *See id.* § 1004.

b. If that were not enough, CALEA gives the Commission no rulemaking authority in the USF context. CALEA applies to *all* telecommunications carriers. *See id.* § 1004 ("A telecommunications carrier . . . ."); *id.* § 1001(8) (definition of a telecommunications carrier). But the principles governing carriers that receive USF funds are set forth in the more specific provisions of 47 U.S.C. § 254. And there is no justification for imposing a requirement under CALEA on just a subset of carriers, because CALEA applies by its very terms to *all* telecommunications carriers, not just those that share some attribute (like USF funding) entirely unrelated to CALEA. *See infra* Part I.D. Indeed, the Commission offers no rationale under which CALEA should be interpreted

to guard against unauthorized surveillance allegedly resulting from use of covered entities' equipment in USF recipients' networks but not use of that same equipment in carriers that do not receive USF. Nothing in CALEA would justify that distinction.

3. CALEA's legislative history likewise undermines the Commission's interpretation

The statute's legislative history makes clear that the purpose of CALEA is to impose requirements on carriers to assist law enforcement and corresponding protections against *law enforcement* abuse. Signal interception can occur almost anywhere, and that was true when CALEA is adopted. It is thus significant that CALEA focuses on "switching premises," because such premises are a place where a carrier employee can provide access for law enforcement, and for which law enforcement needs carrier cooperation. *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: J. Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil & Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 28 (1994) (Mar. 18 Statement of Louis J. Freeh, Director of FBI) ("Since communication interceptions and dialing information acquisitions increasingly will be facilitated from within common carrier premises, including switching facilities and network elements, it is critical that these facilities remain highly secure. . . . [C]ommon carriers will designate individuals who exclusively will have the ability to activate all such interceptions for law enforcement."). Indeed, the legislative history makes clear that government agencies do not have the authority to activate remotely interceptions within the switching premises of a telecommunications carrier: The Commission itself has quoted the legislative history of § 1004, which states that the provision was enacted to "make clear that government agencies do not have the authority to activate remotely interceptions *within the switching premises*

of a telecommunications carrier. Nor may law enforcement enter *onto a telecommunications carrier's switching office premises* to effect an interception without the carrier's prior knowledge and consent when executing a wiretap under exigent or emergency circumstances. . . All executions of court orders or authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier."[4] Similarly, as discussed below, § 229(b)(1) centers on preventing employees from permitting the abuse of the tools CALEA requires carriers to install and maintain as part of ensuring law enforcement's ability to intercept communications.

What is more, the legislative history confirms that even as to law enforcement, § 1004 does not reach communications interceptions that do not occur on carrier "switching premises." *Compare* H.R. Rep. 103-827, at 26 ("All executions of court orders or authorizations requiring access to the switching facilities will be made through individuals authorized and designated by the telecommunications carrier.") *with id.* ("Activation of interception orders or authorizations originating in local loop wiring or cabling can be effected by government personnel"—that is, not on carrier switching premises and not by carrier employees.).

4. The Commission's rulemaking authority under § 229 does not authorize the Draft Order's USF rule either

The Commission also purports to rely on 47 U.S.C. § 229 for the draft rule. Notably, the actual draft rule does not cite § 229 as authority. *Draft Report and Order*, Appendix A. That is not

---

[4] *Communications Assistance for Law Enforcement Act*, CC Docket No. 97-213, Report and Order, 14 FCC Rcd. 4151, 4158, ¶ 17 ("*1999 CALEA Order*") (alterations in original) (emphasis added) (*quoting* H.R. Rep. No. 103-837, at 26 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489), *recon. sua. sponte, Order on Reconsideration*, 15 FCC Rcd. 20735 (2000).

surprising, because § 229(a) merely requires the Commission to "prescribe such rules as are necessary to implement the requirements of [CALEA]"—it does not authorize the Commission to *expand* the requirements of CALEA.

The Commission also points to section § 229(b)(1). That provision states, in full:

> **(b) Systems security and integrity**
>
> The rules prescribed pursuant to subsection (a) shall include rules to implement section 105 of the Communications Assistance for Law Enforcement Act that require common carriers—
>
> (1) to establish appropriate policies and procedures for the supervision and control of its officers and employees—
>
> (A) to require appropriate authorization to activate interception of communications or access to call-identifying information; and
>
> (B) to prevent any such interception or access without such authorization;
>
> (2) to maintain secure and accurate records of any interception or access with or without such authorization; and
>
> (3) to submit to the Commission the policies and procedures adopted to comply with the requirements established under paragraphs (1) and (2).

47 U.S.C. § 229(b)(1).

Section 229(b)(1) by its terms refers to policies and procedures "for the supervision and control of [a carrier's] officers and employees." But the rule here is manifestly not about supervising or controlling officers and employees. Moreover, the rules the Commission prescribes must "implement section 105"—which requires not only authorization for interception of communications, but also "the affirmative intervention of an individual officer or employee of the carrier." *Id.* § 1004. Thus, § 229(b)(1) makes clear that employee involvement helps ensure that interception of communications occurs only with proper authorization.

5. The Commission's interpretation of CALEA is absurd and ignores the Commission's own prior understanding of CALEA

Under the interpretation proposed in the *Draft Report and Order*, as noted, CALEA would require every telecommunications carrier to ensure that no unauthorized interceptions can occur at any "point[] in [its] network where an interception might be activated." In other words, it would interpret the statute as applying to any interception anywhere on a carrier's network, as if the words "effected within its switching premises" were not in the statute. Under this absurd interpretation, a carrier would be liable if (for example) it failed to prevent an unauthorized person from climbing a telephone pole and attaching alligator clips to a pair of copper wires. If an interception "might be activated" at the top of a telephone pole, then that pole becomes a "switching premises" under the proposed interpretation.

Besides twisting the language of the statute beyond recognition, the proposed interpretation ignores past Commission precedent and its own understanding of Congressional intent. In first adopting rules under section 105 of CALEA, the Commission recognized that the primary purpose of this section was to prevent unauthorized interception of communications *by law enforcement agents*.[5] Moreover, the Commission found that commenters in that proceeding "generally agree with our tentative conclusions that section 105 of CALEA imposes a duty upon each carrier to ensure that only lawful interceptions will occur *on its premises*[.]"[6]

The Commission's interpretation of "switching premises" in the *Draft Report and Order* is akin to its interpretation of the term "automatic telephone dialing system" ("ATDS") that was struck down by the D.C. Circuit in 2018 as an unreasonable reading of the Telephone Consumer

---

[5] *1999 CALEA Order*, 14 FCC Rcd. at 4159, ¶ 20 (emphasis added).

[6] *1999 CALEA Order*, 14 FCC Rcd. at 4163, ¶ 27 (emphasis added).

Protection Act ("TCPA").[7] In that case, the D.C. Circuit rejected the Commission's interpretation of "capacity" in the statutory definition of ATDS as encompassing "potential functionalities" and "future possibility,"[8] which the Commission conceded could include smartphones used by everyday Americans. In holding the Commission's reading to be unreasonable, the D.C. Circuit held that "[t]he TCPA cannot reasonably be read to render every smartphone an ATDS subject to the Act's restrictions, such that every smartphone user violates federal law whenever she makes a call or sends a text message without advance consent."[9] The court further proclaimed that "it is untenable to construe the term 'capacity' in the statutory definition of an ATDS in a manner that brings within the definition's fold the most ubiquitous type of phone equipment known, used countless times each day for routine communications by the vast majority of people in the country. It cannot be the case that every uninvited communication from a smartphone infringes federal law, and that nearly every American is a TCPA-violator-in-waiting, if not a violator-in-fact."[10]

So too here, it cannot be the case that section 105 extends to all points of a carrier's network (whether on the carrier's premises or not) where an interception *might* be activated. Just as the Commission's interpretation of ATDS relied too heavily on the theoretical, the Commission's assertion of its authority here relies on potential functionalities and future possibilities. For example,

---

[7] *See ACA Int'l v. FCC*, 885 F.3d 687 (D.C. Cir. 2018).

[8] *ACA Int'l*, 885 F.3d at 695.

[9] *ACA Int'l*, 885 F.3d at 697.

[10] *ACA Int'l*, 885 F.3d at 698.

the Commission cites to the "*possibility*" that untrusted suppliers "will maintain the ability to illegally activate interceptions or other forms of surveillance"[11] but provides no evidence of the likelihood of this possibility occurring or that it has already occurred. Moreover, the Commission's interpretation in the *Draft Report and Order* is inconsistent with 2005 interpretation of "switching" as including "routers, softswitches, and other equipment that may provide addressing and intelligence functions to packet-based communications to manage and direct the communications along to their intended destinations."[12] At that time, the Commission found that this interpretation describes "a function that Congress intended to be covered" and is "most consistent with the purpose of the statute."[13]

The D.C. Circuit in 2018 considered similar disconnects between the legislative history and the Commission's interpretation of ATDS, noting that "a several-fold gulf between congressional findings and a statute's suggested reach can call into doubt the permissibility of the interpretation in consideration."[14] As the court explained,

> "even if the [statute] does not foreclose the Commission's interpretation, the interpretation [can] fall[] outside the bounds of reasonableness" at *Chevron's* second step. *Goldstein v. SEC*, 451 F.3d 873, 880-81 (D.C. Cir. 2006). That is because an "agency['s] construction of a statute cannot survive judicial review if a contested regulation reflects an action that exceeds the agency's authority." *Id*. (quoting *Aid Ass'n for Lutherans v. United States Postal Serv.*, 321 F.3d 1166, 1174 (D.C. Cir. 2003)).[15]

---

[11] *Draft Report and Order*, para. 35.

[12] *2005 CALEA Order*, 20 FCC Rcd. at 14994, para. 11.

[13] *2005 CALEA Order*, 20 FCC Rcd. at 14994, para. 11.

[14] *ACA Int'l*, 885 F.3d at 698.

[15] *ACA Int'l*, 885 F.3d at 698-99.

The court rejected the Commission's ATDS definition, holding that "the Commission's expansive understanding of 'capacity' in the TCPA is incompatible with a statute grounded in concerns about hundreds of thousands of 'solicitors' making 'telemarketing' calls on behalf of tens of thousands of 'businesses'" and that "[t]he Commission's interpretation would extend a law originally aimed to deal with hundreds of thousands of telemarketers into one constraining hundreds of millions of everyday callers."[16] The D.C. Circuit also recalled the Supreme Court's rejection of an interpretation of the term "disability" as used in the Americans with Disabilities Act that would have treated some 160 million persons as disabled in the face of congressional findings contemplating the population of disabled persons as numbering only 43 million.[17]

Similarly, the reach of CALEA – as the *Draft Report and Order* admits – is confined to carriers' "switching premises."[18] However, the *Draft Report and Order* concedes that the definition of "switching premises" adopted for purposes of the instant rule extends well beyond what could reasonably be construed as switching premises and provides the Commission with virtually unlimited regulatory authority to prohibit carriers from using equipment from certain manufacturers under the theory that such equipment could lead to the possibility of illegal interception or other forms of surveillance. Such an expansive reading is at odds with the legislative history of section 105 and CALEA and vastly exceeds the delegation of authority by Congress to the Commission under section 105 and CALEA.

---

[16] *ACA Int'l*, 885 F.3d at 698.

[17] *ACA Int'l*, 885 F.3d at 698 (*citing Sutton v. United Air Lines, Inc.*, 527 U.S.C. 471, 494-95 (1999) (Ginsburg, J., concurring)).

[18] 47 U.S.C. § 1004 (requiring a telecommunications carrier to "ensure that any interception of communications or access to call-identifying information effected *within its switching premises* can be activated only in accordance" with lawful authorization and affirmative intervention by the carrier's officers or employees) (emphasis added).

Unlike the Commission's 2005 interpretation, the interpretation advanced in the *Draft Report and Order* has no meaningful limiting principle and leads to the conclusion that section 105 of CALEA extends to *any point* in all telecommunications carriers' networks. This is an unreasonable and untenable interpretation of section 105.

C. The Commission's Expansive Interpretation of "Switching Premises" Unreasonably and Impermissibly Expands the Reach of CALEA

The Commission's broad view of its authority under section 105 of CALEA also is an unreasonable and impermissible expansion of the scope and reach of CALEA.

Section 103(b)(1) of CALEA denies any law enforcement agency the power "to prohibit the adoption of *any equipment*, facility, service, or feature by any provider of a wire or electronic communication service[.]"[19] The Commission's rulemaking authority under Section 107(b) of CALEA[20] allows it to prescribe standards to "meet the assistance capability standards of [section 103]," but a rule prohibiting carriers from adopting particular equipment is expressly prohibited by Section 103. The Commission cannot reasonably interpret CALEA to authorize a rule that is directly contrary to the specific terms of the statute.

Even if the Commission did have authority to prohibit specific equipment under CALEA, the proposed rule would nonetheless be arbitrary and capricious. The *Draft Report and Order* asserts that the rule implements section 105 of CALEA "by reducing the likelihood that [eligible telecommunications carriers] use USF funds to facilitate unauthorized surveillance."[21] The *Draft Report and Order* relies solely on unsupported speculation that equipment produced by certain

---

[19] 47 USC § 1002(b)(1) (emphasis supplied).

[20] 47 USC § 1006(b).

[21] *Draft Report and Order*, para. 36.

entities results in "the possibility that those suppliers will maintain the ability to illegally activate interceptions or other forms of surveillance within that equipment without the carrier's knowledge, whether through the insertion of malicious hardware or software implants, remote network access maintained by providers of managed services, or otherwise."[22] There is no evidence in the record or otherwise that Huawei equipment has been involved in any unauthorized interception, whether on the networks of USF support recipients or those of other providers. Even if there were such evidence, the Commission's concern with "reducing the likelihood" of such unauthorized surveillance falls short of prohibiting unauthorized interception as is required by section 105.

Indeed, if section 105 of CALEA is interpreted as prohibiting telecommunications carriers from using any equipment that has *any* possibility, no matter how remote, of being subject to unauthorized access for purposes of intercepting communications, then *every* telecommunications carrier is currently in violation of CALEA. There is no such thing as telecommunications equipment that is absolutely secure against unauthorized access under all circumstances. A statutory interpretation that would impose impossible requirements is surely arbitrary and capricious.

D. There is No Nexus Between CALEA and Eligibility for USF Support

Finally, the Commission acknowledges that the rule adopted in the *Draft Report and Order* applies "only to [eligible telecommunications carriers'] use of USF funds" and "disagree[s] with Huawei's argument that the link between this obligation and the prohibition … is 'remote.'"[23] The Commission's position on this point is illogical.

---

[22] *Draft Report and Order*, para. 35.

[23] *Draft Report and Order*, para. 36 (citing Huawei Comments at 31-32).

As the *Draft Report and Order* acknowledges, CALEA (including section 105) imposes obligations on all telecommunications carriers, not just USF recipients.[24] Section 105 was enacted as part of a broader statutory scheme to address concerns regarding the ability for telecommunications carriers to cooperate in the interception of communications for law enforcement purposes as communications evolved to include advanced technologies and features. By contrast, section 254 was adopted to address a specific concern of Congress regarding making advanced communications services available to all Americans. By way of illustration, section 105 does not apply to private networks,[25] which may include Wide Area Networks deployed by schools using support from the E-rate program that would be subject to the rule adopted in the *Draft Report and Order*. Under the statutory interpretation principle that a specific provision governs a more general one,[26] requirements imposed on carriers (and others) participating in the USF program are governed by the specific principles outlined in section 254, not the general provisions of CALEA. Congress

---

[24] *Draft Report and Order*, para. 35 & n. 100.

[25] The term "telecommunications carrier" "(A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier *for hire*; and (B) includes— (i) a person or entity engaged in providing commercial mobile service (as defined in section 332(d) of this title); or (ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter; but (C) does not include— (i) persons or entities insofar as they are engaged in providing information services; and (ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General." 47 U.S.C. § 1001(8).

[26] *See Nitro-Lift Techs. L.L.C. v. Howard*, 568 U.S. 17, 21 (2012) (acknowledging that the interpretive principle that the specific governs the general (*generalia specialibus non derogant*) applies to conflict between laws of equal dignity).

surely did not intend for the Commission to use section 105 to extend its authority over networks and providers that were not intended to be covered by CALEA.

Moreover, if the Commission's position were accurate (which as discussed above, it is not), the Commission ostensibly could dictate what equipment carriers – an even non-carriers that are not subject to CALEA – may use in any network, regardless of whether USF support is used to support the network. This is precisely the type of result that Congress sought to avoid by limiting the ability for law enforcement to dictate the system design of telecommunications carriers subject to CALEA[27] and limiting its application to carriers' switching premises.

II. The Rule and Designation Proceeding Are Unlawful for a Number of Additional Reasons

CALEA aside, the draft rule and proposed designation proceeding are unlawful for several additional reasons:

- The draft rule is not a logical outgrowth of the proposed rule insofar as it relies on invocation of "public safety" under 47 U.S.C. § 254(c)(1)(A). The Commission provided no notice in the NPRM that its proposed rule might rest on a public-safety rationale under § 254(c)(1)(A), and Huawei and other commenters were deprived of the opportunity to contest that reading of the statute or to develop and submit expert testimony on the issue. Yet the Commission now claims that its "decision here to limit the services that will be supported by USF is especially consistent with public safety, under section 254(c)(1)(A)," *Draft Report and Order*, ¶ 31, with no notice or opportunity for comment. In any event, the Commission is wrong on the merits, because § 254(c)(1)(A) gives it no authority for the draft rule.

- Neither the designation process nor the initiation of designation proceedings against Huawei is a logical outgrowth of the proposed rule. The Commission made no proposal in the NPRM about a process for designating companies as "national security

[27] *See* H. Rep. No. 103-837 at 19 (stating that "[t]he bill expressly provides that law enforcement may not dictate system design features and may not bar introduction of new features and technologies" and "establishes a reasonableness standard for compliance of carriers an manufacturers").

threat[s] to the integrity of communications networks or the communications supply chain," *Draft Report and Order*, ¶ 39, yet now purports to create and apply such a process with no notice or opportunity for comment.

- If the draft rule contains any ascertainable criteria for determining whether "a company poses a national security threat to the integrity of communications networks or the communications supply chain," *Draft Report and Order*, ¶ 39, they did not appear in the NPRM and are not a logical outgrowth of the proposed rule; indeed, the NPRM itself noted that, at the time, the FCC had no proposal yet to make about the proper criteria to use. Moreover, since the draft order fails to state meaningful and ascertainable criteria, the rule is in all events void for vagueness: The draft rule gives companies no way of knowing what is required to avoid designation and provides no guidance to ensure that its enforcement is not arbitrary or discriminatory.

- The Commission's draft order is impermissibly retroactive. The order announces a new rule that alters both past and future legal consequences of past actions of Huawei and others—by, among other things, announcing a new legal standard and designating Huawei as in violation of it, because of alleged pre-promulgation conduct and associations, in the same *Draft Report and Order*, with no prior notice, with imposition of serious stigmatic injury, and with disruptive consequences and potential economic and legal exposure from past actions. It is thus both invalid as a "rule" and also "arbitrary and capricious."

- The draft rule is arbitrary and capricious because, among other things, the *Draft Report and Order* fails to address many material comments and proposed alternatives submitted by Huawei and other parties. For example, the Commission failed to respond to the many comments urging it to address the global nature of the supply chain and failed meaningfully to address proposals to adopt a risk-based approach, which would provide greater security while exacting fewer costs.

- The Commission's decision to convert the proceeding from a rulemaking—the only type of proceeding contemplated by the Notice of Proposed *Rulemaking*—to a rulemaking accompanied by an adjudicatory decision (*i.e.*, Huawei's initial designation) is unlawful and prejudicial. Not only is Huawei's designation not a logical outgrowth of the NPRM, but it denies Huawei a meaningful opportunity for comment and pre-deprivation due process. By making such an adjudicatory decision without appropriate notice, the Commission has denied Huawei the opportunity to make a full record for the Commission and the courts. Moreover, neither the proposed rule nor even the initial designation specifies the criteria that will be followed in applying the proposed rule: the proposed rule is silent on the matter and the purported basis for Huawei's initial designation is just an assortment of alleged facts and legal conclusions. As a result, Huawei has not been provided a meaningful opportunity, before the initial designation will take effect, to know what criteria the Commission is relying on, or the standards against which any rebuttal or response will be measured—much less to address the Commission's "facts" or underlying reasoning and/or to provide an appropriate response. In addition, Huawei has had no opportunity to address the harm that such an initial designation will cause to

Huawei, Huawei's reputation, and Huawei's business goodwill. Huawei urges the Commission to remove the initial designation from any final order, and instead to provide Huawei with a meaningful opportunity to be heard and to make an appropriate record on the pertinent issues, and also to provide to Huawei, the Public Safety and Homeland Security Bureau, and all others the criteria upon which a designation is to be based.

- The proposed rule provided no notice regarding what procedural protections the Commission intends to afford initially designated companies, and the *Draft Report and Order* does nothing more than allow Huawei to provide a written submission in response to the accompanying report and initial designation. The Commission did not give Huawei notice of the factual allegations against it or a meaningful opportunity to respond prior to the initial designation, bases the minimal procedures provided on an erroneous understanding of the liberty and property interests at issue, and does not afford Huawei the process to which it is constitutionally entitled for challenging the initial designation. The designation procedures that the Commission has proposed are also legally deficient insofar as they do not foreclose ex parte contacts. *U.S. Lines, Inc. v. Fed. Mar. Comm'n*, 584 F.2d 519, 539-41 (D.C. Cir. 1978); *United States v. Fla. E. Coast Ry. Co.*, 410 U.S. 224, 242-45 (1973). Indeed, Huawei has already explained that it is entitled to the full panoply of protections guaranteed by the Due Process Clause of the Fifth Amendment and the formal adjudication provisions of the Administrative Procedure Act and Communications Act. *See* Huawei Opening Comments 61-86 (June 1, 2018). And even if the Commission denies Huawei these required protections, it is obligated to provide prompt and transparent guidance on the designation proceeding procedures and to indicate with particularity what process will be afforded, for example, to resolve disputed factual issues.

- The designation process that the Commission has proposed is invalid because, among other things, neither the Chief of the Public Safety and Homeland Security Bureau nor any of the Bureau's staff that are responsible for making final designations are properly appointed officers of the United States in accordance with the Appointments Clause of the Constitution, U.S. Const. art. II, § 2, cl. 2. *See generally Lucia v. SEC*, 138 S. Ct. 2044, 2051-55 (2018); *Free Enter. Fund v. Pub. Co. Accounting Oversight Bd.*, 561 U.S. 477, 511-12 (2010).

- Even assuming that an independent agency may constitutionally make national security judgments, the nondelegation doctrine forbids Congress to confer anything more than gap-filling authority on an agency when it delegates law-making power, especially on a policy matter so significant as national security. *See Panama Ref. Co. v. Ryan*, 293 U.S. 388, 426 (1935); *Gundy v. United States*, 139 S. Ct. 2116, 2136-39 (2019) (Gorsuch, J., joined by Roberts, C.J., and Thomas, J., dissenting); *id.* at 2130-31 (Alito, J., concurring in the judgment), *petition for reh'g pending*, No. 17-6086. At a bare minimum, Congress must provide an intelligible principle to guide the agency's actions. *Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 472 (2001). Consequently, under interpretive principles of constitutional avoidance, the Commission may not read 47 U.S.C. § 254 (or any other statute) to give it the power

to place restrictions on USF funds in the name of national security. *See, e.g.*, *Nat'l Cable Television Ass'n, Inc. v. United States*, 415 U.S. 336, 342 (1974) ("the hurdles revealed in [the Supreme Court's nondelegation] decisions lead us to read the Act narrowly to avoid constitutional problems" regarding Congress' delegation of taxing authority to the FCC); *Indus. Union Dep't v. Am. Petroleum Inst.*, 448 U.S. 607, 646 (1980) (plurality opinion) (construing statute to render an agency's interpretation of the statute void in order to avoid a constitutional nondelegation question); *Indus. Union Dep't*, 448 U.S. at 672-76 (Rehnquist, J., concurring in the judgment).

For the foregoing reasons and those stated in Huawei's earlier submissions, the Commission should not adopt the *Draft Report and Order*.

Respectfully submitted,

/s/ Andrew D. Lipman

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

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

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

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

November 14, 2019

Exhibit 22

6/1/2018 Competitive Carriers Association ("CCA") Comments

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

COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION

Steven K. Berry
President & CEO

Rebecca Murphy Thompson
EVP & General Counsel

Courtney Neville
Associate General Counsel

COMPETITIVE CARRIERS ASSOCIATION
601 New Jersey Avenue, NW, Suite 820
Washington, DC 20001
(202) 449-9866
www.ccamobile.org

Theodore B. Olson
Thomas H. Dupree Jr.
Andrew G.I. Kilberg

GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, NW
Washington, DC 20036
(202) 955-8500
www.gibsondunn.com

Counsel for Competitive Carriers Association

June 1, 2018

TABLE OF CONTENTS

I. Introduction and Executive Summary 1

II. The Proposed Rule Will Harm CCA's Members and Millions of Rural Americans. 6

A. The Proposed Rule Will Drive Up Costs by Shrinking the Market and Creating Uncertainty. 6

B. The Proposed Rule Will Reduce Coverage and Degrade Customer Support. 7

C. Carriers Will Be Forced to Rip-and-Replace, Because Mix-and-Match Is Not a Realistic Solution. 9

D. The Proposed Rule Will Deter Carriers from Adopting New Technologies and Investing in Their Networks. 11

E. The Proposed Rule Will Inflict Severe Harm on Rural Consumers. 13

III. The Proposed Rule Exceeds the Commission's Statutory Authority. 15

A. The Proposed Rule Violates Section 254(b)'s Principles. 16

B. The Commission Cannot Rely on Its Authority to Define Universal Service to Impose an Equipment Vendor Mandate. 24

C. Other Statutes Support CCA's Reading of the Universal Service Statute. 27

IV. The Proposed Rule Is Flawed in Many Respects. 28

A. The Proposed Rule's Costs Substantially Outweigh Its Benefits. 29

B. The Proposed Rule Singles Out Smaller, Rural Carriers for Discriminatory Treatment, Contrary to the Very Purpose of the Universal Service Fund. 35

C. The Commission Has Not Identified Evidence Supporting Its Proposed Rule, Nor Has It Tailored the Rule to the Asserted Risk. 37

V. The Proposed Rule Is Unconstitutional. 40

A. The Proposed Rule Violates Due Process. 41

B. The Proposed Rule Results in Unconstitutional Regulatory Takings. 42

VI. If the Commission Proceeds with a Rule, It Should Make Substantial Changes to Mitigate the Proposed Rule's Harmful Impact. 44

VII. The FCC Should Issue a Further NPRM with an Updated, More Detailed Proposed Rule. 47

VIII. Conclusion 49

Appendix: Declarations

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF COMPETITIVE CARRIERS ASSOCIATION

I. Introduction and Executive Summary.

Competitive Carriers Association ("CCA")[1] submits these comments on the rule proposed by the Federal Communications Commission ("Commission" or "FCC") to prohibit the use of money distributed from the Universal Service Fund ("USF") "to purchase or obtain any equipment or services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain."[2] The proposed rule is seriously flawed: it will not serve its intended purpose, is both over- and under-inclusive, will gravely impair the ability of wireless providers to serve the needs of low-income, rural, and unserved and underserved communities, and contains constitutional deficiencies.

CCA has taken a leading role in supporting cybersecurity and network security initiatives

---

[1] CCA is the nation's leading association for competitive wireless providers and stakeholders across the United States, including many recipients of critical USF support. CCA's membership includes nearly 100 competitive wireless providers ranging from small, rural carriers serving fewer than 5,000 customers, to regional and national providers serving millions of customers. CCA also represents approximately 200 associate members including vendors and suppliers that provide products and services throughout the mobile communications supply chain.

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

in light of the pressing need to secure the United States' telecommunications networks against hostile foreign actors. For example, CCA is an industry partner and a participating member of the National Coordinating Center for Communications ("NCC") which is part of the Department of Homeland Security ("DHS"). The NCC monitors threats and coordinates action to protect America's telecommunications infrastructure. Along with other industry and federal partners, CCA assists in "the exchange of vulnerability, threat, intrusion, and anomaly information."[3]

CCA cannot, however, support the proposed rule because it will potentially devastate the ability of carriers receiving USF support to continue to provide service to millions of Americans in rural and other high-cost areas, as explained in the attached declarations. Many carriers have built and now maintain their networks with equipment and services provided by companies targeted by the proposed rule. Much of that investment has been made recently to bring networks from 2G and 3G to 4G and to prepare for the transition to 5G. These carriers simply cannot afford the hundreds of millions of dollars necessary to replace and rebuild their networks using only equipment and services from a new list of approved providers. Some carriers will go out of business as a result; others will struggle to survive. The many Americans who depend on these carriers, mostly in rural and remote areas, will either be forced to help subsidize the massive costs of rebuilding—or will lose their access to telecommunications services entirely.

The proposed rule purports to apply only "prospectively." In truth, it will immediately cause devastating retroactive effects. Many carriers cannot operate networks with an inefficient mix of equipment from various networks, or by depending on one vendor to maintain and upgrade equipment supplied by another. The only practicable solution for most carriers is to rip-

---

[3] National Coordinating Center for Communications, U.S. Dep't of Homeland Sec., https://www.dhs.gov/national-coordinating-center-communications (last updated Feb. 14, 2018).

and-replace equipment within their network. The proposed rule works retroactively: it upsets the settled expectations of carriers and destroys the economic value of their investments.

The proposed rule has already sent a chill of uncertainty throughout the market. This uncertainty deters investment, as carriers will not spend capital on projects that may instantly be rendered worthless if a single component in a long supply chain is placed on the prohibited list. Carriers do not know which foreign companies will be prohibited under the proposed rule, let alone which companies may be added to the list in future years. With such dire consequences for guessing wrongly, including investing in equipment from a company that is permitted today but may be prohibited tomorrow, planned investments will be postponed or abandoned.

Nor does the proposed rule apply equally to all carriers. Rather, it singles out for special restrictions only those carriers who receive USF support—the very carriers that can least afford to rip out and rebuild their networks. While the rule purports to aim at foreign companies whose equipment or services pose a national security threat, the actual, immediate victims will be the millions of Americans who live in rural or unserved and underserved areas and depend on carriers who in turn depend on USF support. The Commission's approach will cause irreparable and immeasurable harm.

As Congress and the Commission have recognized, USF support plays a critical role in connecting rural America to the twenty-first century economy. Consumers today enjoy telecommunications and information services far beyond anything they could have imagined not long ago. The rapid expansion of the nation's networks and the steady development of new technologies allow for faster and more consistent connectivity, giving all Americans access to commercial, educational, medical, entertainment, and other services and products that until recently were difficult to obtain in many parts of the country. Congress, in creating the USF,

deserves credit for this success story. Over its more than two decades of existence, the USF has provided critical support for telecommunications access for rural and other unserved and underserved communities. The USF also aids healthcare providers in rural America, connects students with educational opportunities, and provides subsidies for low-income Americans who might otherwise be disconnected from the modern world. The USF has thus helped the Commission fulfill its statutory mission to "make available, so far as possible, to all the people of the United States . . . a rapid, efficient, Nation-wide, and world-wide . . . communication service with adequate facilities at reasonable charges."[4]

The proposed rule threatens all of this. It will turn the universal service statute and its core principles upside down. Whereas Congress created the USF mechanism as a way to ***provide*** affordable network access to rural America, the proposed rule will use the USF mechanism as a way to ***withdraw*** that access. Congress directed the Commission to administer the USF in accordance with a list of universal service principles. None of those principles are compatible with this rulemaking.

The Commission has provided virtually no evidence supporting its proposed rule, let alone evidence that justifies the proposed rule's draconian effects. Rather, the proposed rule is largely based on a 2012 House Committee report—a very thin justification for a rule that threatens to upend an industry. The Commission does not explain why it waited six years to act if the danger is sufficiently urgent as to effectively require the shutdown of networks. Nor does the Commission explain why a report that focuses on equipment provided by certain vendors should be extended to maintenance services—or why the Commission's proposed prohibition

---

[4] 47 U.S.C. § 151.

goes well beyond the narrow recommendations of the Committee report. The NPRM makes no meaningful effort to assess costs and benefits, presumably because the costs are immense while (as the Commission admits) it does not even know and cannot begin to describe how the benefits might be quantified. Indeed, the NPRM provides little evidence that the proposed rule will make America's vast telecommunications networks any safer, especially since the proposed rule targets only a sliver of those networks—those that rely upon USF funding. Securing the nation's telecommunications networks is vitally important. But vague incantations or appeals to national security cannot override the limits of agency authority, the need for reasoned decision-making, and the requirement that an agency support its conclusions with record evidence.

Other federal agencies are better positioned to make judgments as to how best protect the supply chain from national security threats. The Commission should stay its hand and allow DHS and/or the Department of Commerce ("DoC") to make these expert judgments rather than to thrust itself imprudently into this area. It is ill-advised for the Commission to attempt to make complex national security and foreign policy determinations—areas that are outside the Commission's area of expertise—under the artificial cloak of a USF-eligibility regulation. There must be a rational process to approach national security threats to properly combat them.

At a minimum, the Commission should consider a rule that narrows the scope to limit the harm to carriers and rural Americans and provide a meaningful and robust waiver process. It should not require full compliance for ten years from the rule's adoption to allow carriers sufficient time to reconfigure their networks and spread out costs. And it should establish a compensation fund to mitigate the taking of the carriers' private property and the destruction of their reasonable investment-backed expectations.

II. The Proposed Rule Will Harm CCA's Members and Millions of Rural Americans.

A. The Proposed Rule Will Drive Up Costs by Shrinking the Market and Creating Uncertainty.

Carriers serving rural Americans face difficult challenges. Equipment is more expensive because supply is limited and transportation costs are greater. Smaller carriers struggle to obtain the newest handsets. Services often can be more expensive for similar reasons. Sources of capital are limited. There are currently only two specialty lenders, CoBank and Rural Telephone Financial Cooperative, that possess the understanding of the rural wireless industry needed to properly evaluate the merits of any project financing proposal. For all these reasons, rural areas inherently present higher costs of doing business.

The proposed rule will fundamentally alter the marketplace to the detriment of rural carriers and their customers, as discussed in the individual declarations attached to these comments.[5] The proposed rule threatens to drastically alter the supplier market for core network equipment. The number of suppliers of services also will be cut significantly. The relative cost of both replacement and next-generation equipment will rise as a result of the proposed rule, as will the cost of borrowing. Lower-cost providers will be pushed out of the market, which will reduce overall supply and increase demand for the higher-cost providers. Elimination of lower-cost competitors will increase wholesale costs from other manufacturers for both network infrastructure equipment and devices by removing a key constraint on pricing.

---

[5] Decl. of Steven K. Berry (June 1, 2018); Decl. of Michael Beehn (June 1, 2018); Decl. of Frank DiRico (June 1, 2018); Decl. of James Groft (May 29, 2018); Decl. of Todd Houseman (June 1, 2018); Decl of Michael D. Kilgore (June 1, 2018); Decl. of John C. Nettles (June 1, 2018); Decl. of Eric J. Woody (June 1, 2018).

The proposed rule will introduce (in fact, already has introduced) substantial uncertainty into the markets for network equipment, devices, and services because carriers cannot predict whether companies that are approved today might be deemed suspect tomorrow, or whether the market can withstand the elimination of a substantial portion of suppliers. Uncertainty leads to higher upfront and ongoing costs, as well as lost revenue from foregone investments. Instead, the FCC must attempt to develop demonstrable improvements in its national security, rather than propose detrimental regulatory burdens on carriers with no clear benefit. Chairman Pai has expressed grave concern over just this type of problem in the context of the 2016 budget control mechanism.[6] Higher costs caused by the proposed rule will combine with cuts in USF support overall.[7] And, of course, higher costs likely mean higher rates for consumers. Moreover, customer churn or loss rate will increase, which pushes the direct-to-consumer harms back onto the carriers, creating a dangerous cycle.

B. The Proposed Rule Will Reduce Coverage and Degrade Customer Support.

Of vital importance to carriers is the quality and timeliness of the services provided by equipment vendors, many of whom operate under long-term or opt-in extension contracts. Rural carriers serve fewer customers, who are spread across a wider geographic area. The market

---

[6] *See* Press Release, Federal Communications Commission, Statement of Chairman Ajit Pai on Projected USF Budget Cuts for Small, Rural Carriers (May 1, 2018).

[7] *See Connect America Fund; A National Broadband Plan for Our Future; Establishing Just and Reasonable Rates for Local Exchange Carriers; High-Cost Universal Service Support; Developing an Unified Intercarrier Compensation Regime; Federal-State Joint Board on Universal Service; Lifeline and Link-Up; Universal Service Reform – Mobility Fund*, WC Docket No. 10-90, GN Docket No. 09-51, WC Docket No. 07-135, WC Docket No. 05-337, CC Docket No. 01-92, CC Docket No. 96-45, WC Docket No. 03-109, WT Docket No. 10-208, Report and Order and Further Notice of Proposed Rulemaking, 26 FCC Rcd 17672, ¶ 18 (2011) (*USF/ICC Transformation Order*) (announcing budget cap mechanism for high-cost USF program).

reality is that companies providing services such as repairs and equipment installations prioritize larger carriers with more urban and suburban footprints. For example, in 2017, one CCA member experienced a network outage that lasted more than 24 hours because the carrier could not get the vendor to service the carrier's equipment. The experience of many rural carriers has been that newer foreign entrants to the market for these services are more attentive to rural carriers than other service-providers and perform repairs and installations more quickly and reliably. The quality and timeliness of these services increase coverage reliability for consumers, including subscribers to larger carriers who use rural networks while roaming. That reliability, in turn, supports expansion of the Internet- and app-based economy into rural areas and enhances public safety by ensuring access to emergency services.

Support for consumer devices also is critical. Devices and the operating systems ("OS") and applications that populate them require software updates on a regular basis. OS and application updates are developed, tested, and deployed in multistep processes that rely on several entities located around the world. An OS provider in the United States, for example, may identify an issue that necessitates an update, which has to be developed and made available to manufacturers who customize the OS for their devices. Those updates often are tested by the network operator and may be sent back for further development by the manufacturer or the OS developer. These functions may be supported by companies that may at some time in the process be on the prohibited list. If an application is unable to download and install updates, the application eventually will not work. The same is true of the phones and tablets themselves. Without critical software updates, a device eventually becomes unusable. And even before that point is reached, the device becomes vulnerable to malicious malware and hacking attempts because it lacks the most recent security software updates. Because many CCA members receive

USF support to upgrade and maintain their networks, it is possible that consumer devices will be unable to access the software updates that these devices require.

C. Carriers Will Be Forced to Rip-and-Replace, Because Mix-and-Match Is Not a Realistic Solution.

The proposed rule will result in many carriers having to rip out and replace all equipment bought from companies that are on or become placed upon the list of banned entities, because that equipment will become unusable in a short period of time without upgrades and services. Carriers could try to use new service providers to work on old equipment and install upgrades manufactured by different companies. But there is great uncertainty as to whether existing network equipment purchased from now-disapproved manufacturers can interoperate or function with new equipment from approved vendors. Carriers theoretically could attempt to plug upgrade or necessary replacement equipment from an approved manufacturer into clusters of equipment sourced from a disapproved company, but even if it works in the short term, the mid- and long-term viability of that arrangement and even the short-term performance efficiency remain highly uncertain. Many carriers thus will be forced to rip and replace their network equipment to stay competitive in today's marketplace—a business environment in which consistent performance is essential.

Perhaps more importantly, replacement service vendors require full access to all prior software code to ensure that the legacy equipment continues to function. But obtaining full access will likely be impossible. Software is proprietary and upgrades, patches, and other maintenance cannot be obtained unless and until it is licensed by the vendor of that software—in this case, the company with which transactions are proposed to be prohibited. The core also will likely need to be replaced, which exacerbates the compatibility problem for existing area equipment. There is little a third party can do. For example, one CCA member undertook

network migration from a non-Chinese-based vendor to a Chinese-based vendor, and in so doing, experienced equipment interoperability challenges that led to a network outage. The reality, therefore, is that even though the FCC intends its proposed rule to operate prospectively, it will have devastating and immediate retroactive effects.

Additionally, the level of pre-deployment testing that must be done to meet legitimate service expectations for new products requires significant research and development costs. Those costs must be absorbed if carriers rip and replace network equipment. They also must be incurred if a carrier were to attempt to cobble together a mix-and-match network—without any real guarantee that a hodgepodge and shifting network infrastructure with new service providers can continue to meet service expectations in an uncontrolled environment. Even if research and development costs could be recovered, various "most favored nation" clauses in purchase contracts often place hard limits on pricing offered to smaller carriers.

Implementation of the proposed rule will cause immense financial harm to carriers. For example, one small- to mid-sized carrier with approximately 100,000 subscribers has estimated that the cost to replace all network equipment—including core, fiber, microwave, and wireless equipment—could approach $300 million, which is three times the amount that the current vendor would charge for the same equipment. In addition, the carrier will have to spend $60 million more for services. Finally, downtime from installing new equipment would cause the company to forego at least $50 million in roaming fees. This ***single carrier*** estimates that it will likely lose approximately $410 million if the proposed rule is adopted.[8]

---

[8] *See* Decl. of Frank DiRico 3.

Many other carriers will suffer similarly catastrophic consequences to their financial viability. For example, one small carrier estimates a roughly $100 million replacement cost for its network equipment alone, not including the cost of any additional services that will be required. The carrier also will risk nearly $2 million in lost revenue from government contracts, nearly $26 million of lost revenue from roaming arrangements, and approximately $20 million of lost USF support annually during the transition from Huawei to a new supplier. This would be devastating to the carrier's business.[9] Another CCA member serving just over 100,000 customers estimates nearly $310 million in costs for new core and related equipment, an additional $60 million in costs for services and maintenance, and a loss of approximately $40 million in roaming revenue.

D. The Proposed Rule Will Deter Carriers from Adopting New Technologies and Investing in Their Networks.

The proposed rule will slow down or even entirely prevent adoption and integration of new technologies, such as 5G wireless capability, which runs counter to the FCC's stated priorities.[10] CCA's members consistently provide wireless broadband access through their 4G networks and have made substantial progress in building out their 4G VoLTE capabilities. They have begun planning and testing for the eventual transition to 5G technology. Capital that would otherwise be put toward achieving the next generation of technology instead will be spent replacing current equipment. This trend is already evident: capital investments by CCA's

---

[9] *See* Decl. of Eric J. Woody 2–3.

[10] *See, e.g.*, *Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment*, WT Docket No. 17-79, Second Report and Order, ¶ 4–5 (rel. Mar. 30, 2018) (discussing FCC's "efforts to reduce regulatory impediments" to "promot[e] this country's leadership in 5G").

carrier members declined precipitously in the first quarter of 2018, in large part because of anticipated tighter restrictions on carriers' access to equipment and services provided by certain foreign companies. At the current pace, for example, one of CCA's members is on track to invest approximately $10,000 in network expansion in the first quarter of 2018. That same carrier invested over $5.3 million in network expansion in 2017 and over $5 million per year on average between 2012 and 2017. Uncertainty as to the next arbitrary regulation will restrict providers and investors from making long-term investments.

As another example, one CCA carrier member began installation of a new base station in a small southern town with a population of 26. However, due to recent actions by the administration, the member's vendor company has declined to complete software updates or to transfer software licenses, and the member has been unable to turn on LTE service as a result. That same CCA member has three more base stations which are scheduled to be deployed to provide wireless broadband services to other low-density areas where broadband service from the incumbent wireline carrier is unavailable or inadequate. However, the ability to complete that work will be stalled for the same licensing issue and fear of penalty. And another CCA carrier member reports that it has abruptly had to halt deployment for numerous additional coverage areas that were planned to occur over the next 12 to 24 months.

CCA members pride themselves on serving consumers in rural and remote areas, which are often the communities where the owners and employees of these carriers live and work, in no small part because serving rural and remote areas saves lives. One CCA member serving portions of rural Nevada deployed a cell tower in Death Valley National Park in Nevada. As a result of this carrier's efforts, "two French nationals, a 27-year-old man and a 21-year-old woman, were rescued from extreme heat . . . after making a phone call that may not have

connected before this cell tower was installed."[11] And when a small plane crashed in rural Wyoming, passengers were able to contact first responders because a small carrier whose network relies on Chinese equipment serves the remote area where the plane went down. Services from these two carriers offered the only area of coverage in otherwise "dead" zones. Looking forward, the FCC's proposed actions in this proceeding ultimately will stunt network expansion measures and will further expand the digital divide in rural areas.

E. The Proposed Rule Will Inflict Severe Harm on Rural Consumers.

The proposed rule will harm consumers, particularly those living in rural areas. Coverage outages will proliferate as a result of some carriers shutting down and others going temporarily offline to replace equipment and perform the pre-deployment testing that must take place beforehand. In addition, replacement, maintenance, and repair services likely will be slower to respond, which could cause more frequent and longer outages. Those coverage voids are not mere annoyances. It is undisputable that "[h]igh-speed Internet access, or broadband, is critical to economic opportunity, job creation, education, and civic engagement."[12] Coverage disruptions hinder business transactions, including small businesses trying to process credit card

---

[11] "New Cell Tower Helps Save Three Lives in Death Valley," Sierra Wave Media, https://www.sierrawave.net/new-cell-tower-helps-save-three-lives-in-death-valley/ (July 21, 2010).

[12] Federal Communications Commission, *Bridging The Digital Divide For All Americans*, https://www.fcc.gov/about-fcc/fcc-initiatives/bridging-digital-divide-all-americans (last visited May 28, 2018). *See also*, Accenture, "How the Wireless Industry Powers the U.S. Economy" – A Study Commissioned by CTIA (rel. Apr. 5, 2018), *available at* https://www.ctia.org/news/study-reveals-powerful-economic-impact-of-wireless-across-50-states (noting, the "U.S. wireless industry contributes $475 billion annually to America's economy and supports 4.7 million jobs").

payments; frustrate classroom curricula; and simply prevent people from connecting with each other. The time and capital carriers will have to spend addressing these problems will frustrate their ability to plan for and invest in 5G. Rural Americans must not be relegated to second-class status when it comes to communications access.[13]

Consumers will not only lose coverage, but also will be unable to update their devices. The inability to update devices will make the network ***less*** secure as consumers would be unable to get critical security software updates—a very serious risk in a constantly evolving cybersecurity landscape.

In sum, the proposed rule's effects on telecommunications and information services access for underserved communities, especially rural areas, will be calamitous. It will take a decade or more to recover. During that time, the rest of the country and the rest of the world will continue to innovate in network and device technology, invest in those systems and support services, and improve the speed and quality of connectivity. All the while, rural America will fall further and further behind. This is not what Congress envisioned in 1934 when it created the FCC, nor in 1996 when it modernized the support system for high-cost areas and other underserved communities and institutions. Nor is it consistent with the Commission's stated priorities.

---

[13] *See id.* ("Chairman Ajit Pai's top priority is to close the digital divide between those who have access to cutting-edge communications services and those who do not. He believes that every American who wants to participate in the digital economy should be able to do so.").

III. The Proposed Rule Exceeds the Commission's Statutory Authority.

The Commission claims that Sections 201 and 254 of the Communications Act "provide ample legal authority" for the proposed rule.[14] In the Commission's view, Section 201(b)'s grant of general rulemaking authority, and Section 254(e)'s direction that USF dollars shall be used "only for the provision, maintenance, and upgrading of facilities and services for which the support is intended," give the Commission the authority to institute an equipment vendor mandate.[15] The Commission also asserts that Congress's direction in § 254(c)(1) that the Commission should "periodically" update "the definition of the services that are supported by" the USF gives it the authority to issue the proposed rule because national security is an important "public interest."[16]

None of this is correct. The Commission's general rulemaking authority must be exercised in accordance with the "[u]niversal service principles" set forth in Section 254(b). The proposed rule, however, ***conflicts*** with these principles. Whereas the principles emphasize the importance of preserving and expanding service for Americans in rural or underserved areas, the proposed rule will restrict and, in some cases, eliminate service for the very people the universal service mandate is intended to protect. Nor can the proposed rule be justified as a "re-definition" of universal service. The FCC's obligation to consider "the public interest" in defining universal service[17] does not authorize the Commission to ignore or override the universal service

---

[14] NPRM ¶ 35.

[15] *Id*.

[16] *Id*. ¶ 36.

[17] 47 U.S.C. § 254(c)(1)(D)

principles set forth by Congress in Section 254(b). The FCC's proposed rule, if adopted, will exceed the Commission's statutory authority and thus will violate the APA.[18]

A. The Proposed Rule Violates Section 254(b)'s Principles.

Congress directed the Commission to base its universal service rules on an enumerated list of policy principles. Section 254(b) provides that "the Commission ***shall*** base policies for the preservation and advancement of universal service on [specified] principles" (emphasis added). As the Tenth Circuit has explained, "[t]he plain text of the statute mandates that the FCC 'shall' base its universal policies on the principles listed in § 254(b). This language indicates a mandatory duty on the FCC."[19] The specificity of Section 254(b) unquestionably controls over Section 201(b)'s general grant of rulemaking authority.[20]

Although the Commission identifies some of the universal service principles codified in Section 254(b),[21] the NPRM does not explain how the proposed rule furthers those principles. No doubt that is because the proposed rule—which will limit and, in some cases, cut off service to rural and underserved Americans—plainly undercuts and frustrates those principles. A rule that restricts or eliminates universal service indisputably conflicts with Section 254's mandate that FCC rules "preserve and advance" universal service.

As discussed above, the proposed rule will cause massive service disruptions in high-cost, rural areas and could result in higher consumer rates to attempt to offset the costs of replacing equipment and services currently provided by the targeted companies. Consumers who

---

[18] *See* 5 U.S.C. § 706(2)(A), (C) (agency action must be set aside if it is "not in accordance with law" or "in excess of statutory jurisdiction, authority, or limitations").

[19] *Qwest Corp. v. FCC*, 258 F.3d 1191, 1200 (10th Cir. 2001) ("*Qwest I*").

[20] *Gozlon-Peretz v. United States*, 498 U.S. 395, 407 (1991).

[21] *See* NPRM ¶ 35

own phones and other devices manufactured by those companies will also be deprived of the ability to download critical software updates. The proposed rule will thus increase costs and reduce access to telecommunications and information services in the very places the USF was intended to support. Although network security is important, forcing rural carriers out of business "throws the baby out with the bathwater." Services are not "preserved" because consumer access will be reduced from current levels. And services are not "advanced" because investment, expansion, and growth will be chilled and discouraged. "The use of the conjunctive 'and' in the phrase 'preserve and advance universal service,' or 'preservation and advancement of universal service,' clearly indicates that the Commission cannot satisfy the statutory mandate by simply doing one or the other."[22] The proposed rule does neither.

The proposed rule directly conflicts with every principle set forth in Section 254:

- Subsection (b)(1) – "Quality and rates." By requiring USF-supported carriers to rebuild their networks at immense expense, the proposed rule will drive up rates without a proportionate increase in quality. This violates the principle that "[q]uality services should be available at just, reasonable, and affordable rates."
- Subsection (b)(2) – "Access to advanced services." Whereas Congress emphasized the need for "[a]ccess to advanced telecommunications and information services . . . in all regions of the Nation," the proposed rule will have the effect of curtailing access to such services in rural and other areas of the nation with low population density. The FCC has reinforced the importance of this principle by expressly

---

[22] *Qwest Comms. Int'l, Inc. v. FCC*, 398 F.3d 1222, 1236 (10th Cir. 2005) ("*Qwest II*").

adopting "Support for Advanced Services" as an additional principle, which instructs the Commission to "direct[ ]" USF funds "where possible to networks that provide advanced services, as well as voice services."[23]

- Subsection (b)(3) – "Access in rural and high cost areas." The proposed rule will have a devastating effect on the services available to Americans in rural and high cost areas. Under the proposed rule, low-income Americans, and persons living in rural or high cost areas will ***not*** have services "that are reasonably comparable to those services provided in urban areas and that are available at rates that are reasonably comparable to rates charged for similar services in urban areas."
- Subsection (b)(4) – "Equitable and nondiscriminatory contributions." The proposed rule blatantly violates this principle by forcing USF-supported carriers—and ***only*** USF-supported carriers—to remove the equipment, and forego the services, at issue. Singling out USF-supported carriers for inequitable and discriminatory treatment directly conflicts with the congressional judgment that "***[a]ll*** providers of telecommunications services should make an equitable and nondiscriminatory contribution to the preservation and advancement of universal service" (emphasis added).
- Subsection (b)(5) – "Specific and predictable support mechanisms." The proposed rule is anything but "specific" and "predictable." It imposes a broad, vague, and uncertain mandate that upsets settled expectations and makes investment planning virtually impossible, as companies lack the knowledge to foresee which companies

---

[23] *USF/ICC Transformation Order*, 26 FCC Rcd 17679, ¶ 45.

could get added to the list of prohibited vendors. Beyond the clear suggestion that ZTE and Huawei will be placed on the list, it is far from clear what other companies might qualify for inclusion. Carriers will hesitate to invest in network equipment or devices that could end up prohibited on short notice, a reality already illustrated by the dramatically reduced investment in network expansion.

- Subsection (b)(6) – "Access to advanced telecommunications services for schools, health care, and libraries." By jeopardizing the continued provision of service to rural and underserved areas, the proposed rule threatens the ability of "schools and classrooms, health care providers, and libraries [to] access . . . advanced telecommunications services."

Because the proposed rule so clearly violates these six enumerated principles, the NPRM sidesteps any discussion of them and instead notes subsection (b)(7)'s language that the Commission may be guided by "[s]uch other principles as the Joint Board and the Commission determine are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter." But this provision cannot justify the proposed rule.

First, the Commission's vague articulation of the "public interest" cannot override the six specified principles in Section 254. Although the Commission "may exercise its discretion to balance the principles against one another when they conflict," it "may not depart from them altogether to achieve some other goal."[24] Here, the Commission will be departing from all six specified principles to achieve a goal that is ***not*** specified in Section 254.

---

[24] *Qwest I*, 258 F.3d at 1200.

Second, if the Commission wishes to recognize a new principle using its subsection (b)(7) authority, it must first obtain a determination by the Federal-State Joint Board that the principle is "necessary and appropriate."[25] That determination can only be made through a notice-and-comment proceeding.[26]

Third, it is neither "necessary" nor "appropriate" to single out network security as a universal service principle. It is not "necessary" because other agencies, such as DHS or DoC, are far better positioned to assess the national security risks posed by individual companies—and those agencies have a variety of ways to address the relevant risks. The Commission has declined to regulate in analogous circumstances.[27] And as the Supreme Court has cautioned quite recently, one agency will not receive deference if its interpretation of a statute "limits the work of a second statute" administered by a separate agency.[28] The FCC's work could ultimately curtail or cut short these agencies' due diligence. In this context, the FCC should allow other expert agencies to take the lead.

DHS is, in fact, currently assessing telecommunications supply chain risks. The National Protections and Program Directorate is expected to release a multi-faceted report by the end of summer 2018. The report likely will assess the telecommunication industry's risk for hardware,

---

[25] *See* 47 U.S.C. § 254(b)(7) (allowing adoption of "[s]uch other principles as the Joint Board ***and*** the Commission determine are necessary and appropriate" (emphasis added)).

[26] *See Federal-State Joint Board on Universal Service*, CC Docket No. 96-45, Report & Order, 12 FCC Rcd. 8799–806, ¶¶ 43–55 (rel. May 8, 1997) (considering and discussing comments on whether to adopt a new universal service principle).

[27] *See Restoring Internet Freedom*, WC Docket No. 17-108, Declaratory Ruling, Report & Order, & Order, ¶¶ 140, 143–52 (rel. Jan. 4, 2018) ("*Restoring Internet Freedom* Order") (relying on sufficiency of antitrust law in addressing "conduct that harms Internet openness" as reason to repeal "net neutrality" order).

[28] *Epic Systems Corp. v. Lewis*, No. 16-285, slip op. at 20 (May 21, 2018).

software, and services, as well as perform targeted risk assessments based on specific threats, vulnerabilities, or entities at risk. The report likely also will examine specific threats to manufacturers, software designers, service providers, and hardware and software vulnerabilities within all sectors of the American telecommunications ecosystem.

This top-to-bottom assessment is viewed as part of a larger cybersecurity strategy aimed at protecting critical infrastructure, especially that which has become integrated with the internet. DHS identifies 16 sectors of critical infrastructure in the United States including communications and information technology.[29] On May 15, 2018, DHS released its cybersecurity strategy, noting "[b]y 2023, the Department of Homeland Security will have improved national cybersecurity risk management by increasing security and resilience across government networks and critical infrastructure; decreasing illicit cyber activity; improving responses to cyber incidents; and fostering a more secure and reliable cyber ecosystem through a unified departmental approach, strong leadership, and close partnership with other federal and nonfederal entities."[30] DHS plans to assess each of the 16 critical infrastructure sectors with a clearly defined strategic approach.

Further, DoC is already addressing supply chain risks. The agency is using its tools and authorities to take action against those companies it deems bad actors and security risks. In fact, DoC's April 15, 2018, Denial Order against ZTE has had serious impacts and is still being reviewed. The complexity and fluidity of that situation illustrates how ill-suited the FCC is to wade into complex security and trade issues. Excluding a company from U.S. markets can have

---

[29] Office of Infrastructure Protection, U.S. Dep't of Homeland Sec., *Critical Infrastructure Sectors*, https://www.dhs.gov/critical-infrastructure-sectors (last updated July 11, 2017).

[30] U.S. Dep't of Homeland Sec., Cybersecurity Strategy (May 15, 2018), *available at* https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

serious diplomatic consequences that the FCC and the Universal Service Administrative Company are not well positioned to anticipate or nimbly manage.

In addition to not being "necessary," recognizing network security as a universal service principle is not "appropriate," because it has the effect of singling out universal service recipients for discriminatory treatment. Confining the restriction to USF recipients is harmful to rural and regional carriers and the millions of Americans who rely on them. A discriminatory punitive sanction of this nature is not "appropriate," especially when the Commission can regulate more comprehensively.

It is more appropriate for DHS, rather than the FCC, to take the lead on issues pertaining to the national supply chain and national security. DHS is equipped with the necessary staff with required security clearances, internal infrastructure, critical expertise, and designated authority to thoroughly and thoughtfully determine risks and vulnerabilities within the telecommunications supply chain as well as any threats to national security that may arise. DHS can work with the intelligence community and process shared information about critical infrastructure risks far more ably than the Commission. The FCC should defer to DHS, and if helpful, provide technical expertise. For example, the FCC is currently awaiting the advice of its Communications Security, Reliability and Interoperability Council ("CSRIC"), which has a working group examining supply chain security.[31] Heeding these recommendations prior to commencing a rulemaking better reflects the FCC's traditional and prudent practice of convening subject-matter experts to inform Commission policy.

---

[31] *See* NPRM ¶ 9.

Finally, the proposed rule also violates the principle of competitive neutrality. The Commission long ago adopted the competitive neutrality principle pursuant to its Section 254(b)(7) authority.[32] "[C]ompetitive neutrality means that universal service support mechanisms and rules neither unfairly advantage nor disadvantage one provider over another, and neither unfairly favor nor disfavor one technology over another."[33] In that regard, the Commission pledged to "avoid limiting providers of universal service to modes of delivering that service that are . . . not cost effective."[34] This principle "should be considered in formulating universal service policies relating to each and every recipient and contributor to the universal service support mechanisms, regardless of size, status, or geographic location."[35] Competitive neutrality is a bedrock aspect of the USF regime that requires the FCC not to disadvantage one type of carrier.

The NPRM fails even to mention competitive neutrality, much less adhere to it. The proposed order will unfairly disadvantage rural and other USF-supported carriers by eliminating their ability to purchase cost-effective equipment, devices, and services. The many carriers who built their networks by using equipment from targeted companies did so precisely because those companies offered the most cost-effective products and services on the market. In some cases, those companies were effectively the ***only*** available providers of products and services. The

---

[32] *See Federal-State Joint Board on Universal Service*, 12 FCC Rcd. 8779–806, ¶¶ 43–52.

[33] *Id.*, 12 FCC Rcd. 8801, ¶ 47.

[34] *Id.*, 12 FCC Rcd. 8802, ¶ 49.

[35] *Id.*

proposed rule unfairly disadvantages these carriers, thus violating the principle of competitive neutrality.

B. The Commission Cannot Rely on Its Authority to Define Universal Service to Impose an Equipment Vendor Mandate.

The Commission asks whether "adopting [the] proposed rule [will] be equivalent to establishing a new definition of" universal service under its Section 254(c)(1) authority.[36] The answer is no.

"Universal service" refers to a set of telecommunications services that the Commission is statutorily directed to achieve, maintain, and expand. The meaning of universal service is distinct from the individual ***vendors*** who provide the equipment and services that enable carriers to offer telecommunications services to their customers. This common-sense understanding of universal service is evident in the text of the statute itself, which defines universal service as "an evolving level of telecommunications services that the Commission shall establish periodically under this section, taking into account advances in telecommunications and information technologies and services."[37]

The plain meaning of universal service is reinforced by the congressional mandate that "the Commission in establishing the definition of the services that are supported by Federal universal services support mechanisms shall consider the extent to which such telecommunications services are essential to education, public health, or public safety; have, through the operation of market choices by customers, been subscribed to by a substantial

---

[36] NPRM ¶ 36.

[37] 47 U.S.C. § 254(c)(1).

majority of residential customers; are being deployed in public telecommunications networks by telecommunications carriers; and are consistent with the public interest, convenience, and necessity."[38] This language establishes that universal service refers to a suite of services, or a group of specific functionalities, rather than to the ***identity*** of the equipment vendor who provides the technology that enables a carrier to offer these services and functionalities.

The statutory structure confirms this plain meaning. Section 254(b) sets forth the principles that must guide Commission rulemakings addressing universal service, and Section 254(c) gives the Commission authority to "establish periodically" the "evolving level of telecommunications services" that shall constitute universal service. If the Commission could evade the Section 254(b) principles simply by framing a funding restriction as a "re-definition" of universal service, Section 254(b) would be deprived of any constraining force, and its nondiscrimination and access-preservation goals would be rendered a practical nullity.

Even if the Commission could sidestep the clear statutory text and structure, the considerations identified in Section 254(c) cut against the proposed rule. There can be no dispute that the services at issue "are essential to education, public health, [and] public safety;" reflect "the operation of market choices by customers;" and "are being deployed in public telecommunications networks by telecommunications carriers." The NPRM refutes none of this. Instead, the NPRM relies once again on the "public interest" as a purported trump card that can override all other considerations. That is impermissible. The "public interest" factor must be read in harmony with the other factors, all of which underscore that universal service is meant to encompass important telecommunications services that are widely used by consumers in the free

---

[38] *Id*. (internal punctuation and numbering omitted).

market. Invoking the "public interest" factor as way of smuggling in a consideration that is different in kind—network security—would violate the *ejusdem generis* canon, which holds that a final, catch-all item in a list should be read to include only things "of the same sort" as the other, specific items in the list.[39]

Finally, the Commission overreads the Tenth Circuit's statement that "nothing in the statute limits the FCC's authority to place conditions . . . on the use of USF funds." *In re FCC 11-161*, 753 F.3d 1015, 1046 (10th Cir. 2014). That case had nothing to do with—and, thus, did not approve—a rule requiring or prohibiting the use of particular equipment vendors, much less a rule conditioning USF funds on national security determinations. The court's statement, moreover, did not concern whether a particular condition for USF eligibility was consistent with the statute. In fact, the court explained that the Commission's "funding directives" must be "consistent with the principles" enumerated by Congress in Section 254(b).[40] The court also noted that the Commission itself defended its regulation on the ground that it may "create inducements . . . to ensure that the universal service policies outlined in Section 254(b) are achieved."[41] The Tenth Circuit's decision thus confirms that Commission rules and policies cannot conflict with the principles set forth in Section 254(b).[42]

---

[39] *See* Scalia & Garner, *Reading Law* 199–200 (2012); *see Epic Systems*, No. 16-285, slip op. at 12.

[40] *In re FCC 11-161*, 753 F.3d at 1047.

[41] *Id*. at 1045.

[42] The Tenth Circuit also held that it was reasonable for the FCC to interpret Section 254(e)'s reference to the use of USF funds to support "facilities" as authority "to encourage the types of facilities that will best achieve the principles set forth in section 254(b)." *Id.* at 1046–47. But even a capacious reading of "facilities" cannot support a mandate that USF recipients contract only with specific vendors of equipment and services.

If the FCC were to move forward with re-defining "universal service" through its Section 254(c) authority, it first must submit the matter to the Joint Board for consideration and may adopt a new definition only if the Board has recommended that it do so. Under Section 254(c)(1), it is the Joint Board's responsibility to first "recommend[ ] . . . the definition of the services that are supported by" the USF. And Section 254(c)(2) confirms that the "Joint Board may, from time to time, recommend to the Commission modifications in the definition of the services that are supported by Federal universal service support mechanisms." The statute is clear that the Commission cannot re-define "universal service" unless it works through and with the Joint Board.

C. Other Statutes Support CCA's Reading of the Universal Service Statute.

Congress has repeatedly codified its policy of encouraging universal access to advanced telecommunications and information services through pro-competitive and deregulatory methods. In 1934, Congress created the FCC "[f]or the purpose" of "mak[ing] available, so far as possible, to ***all*** the people of the United States . . . a rapid, efficient, Nation-wide, and world-wide . . . communication service with adequate facilities at reasonable charges."[43] Congress has instructed the Commission "to promote the continued development of the Internet and other interactive computer services" while "preserv[ing] the vibrant and competitive free market that presently exists."[44] Section 706(a) of the Telecommunications Act, furthermore, directs the Commission to

---

[43] 47 U.S.C. § 151 (emphasis added).

[44] 47 U.S.C. § 230(b).

> encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to ***all*** Americans . . . by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, ***measures that promote competition*** in the local telecommunications market, or other regulating methods that ***remove barriers to infrastructure investment***.[45]

If that were not clear on its own, Section 706(b) of the Telecommunications Act tells the Commission to "determine whether advanced telecommunications capability is being deployed to ***all Americans*** in a reasonable and timely fashion," and, if it is not, to "take immediate action to accelerate deployment of such capability by ***removing barriers to infrastructure investment*** and by ***promoting competition*** in the telecommunications market."[46] As the Commission has recently explained, these provisions "exhort[ ] the Commission to exercise market-based or deregulatory authority granted under other statutory provisions" to support universal service.[47]

By eliminating a major part of the market for lower-priced network equipment and services, however, the proposed rule contravenes Congress' clearly stated policy. The proposed rule stifles competition and promotes conglomeration throughout the supply chain. It will eliminate access for many rural Americans—and increase prices and reduce market choices for everyone else.

IV. The Proposed Rule Is Flawed in Many Respects.

There are other serious deficiencies in the proposed rule that render it invalid under the Administrative Procedure Act.[48] Among other things, the immense costs of the rule massively

---

[45] 47 U.S.C. § 1302(a) (emphases added).

[46] 47 U.S.C. § 1302(b) (emphases added).

[47] *Restoring Internet Freedom* Order, ¶ 270.

[48] *See* 5 U.S.C. § 706(2)(A) (agency action must be set aside if it is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law").

outweigh the unspecified benefits; the rule unfairly singles out and discriminates against USF-supported carriers, contrary to the USF's purpose; and even assuming the importance of securing the supply chain, the Commission has failed to tailor the rule to the danger at issue. The Commission's approach is directly contrary to the President's emphasis on reducing the regulatory burden on private business.[49]

A. The Proposed Rule's Costs Substantially Outweigh Its Benefits.

1. The Commission must give "at least some attention to cost" in all of its rulemakings.[50] That requirement is embedded within the Commission's general rulemaking power as well as the "public interest" provisions the Commission cites as the authority for this rulemaking.[51] Moreover, Congress has required the Commission to administer the USF pursuant to the policies enumerated in Section 254(b). Those policies emphasize ensuring the affordability of access and providing sufficient financial support to carriers serving rural and high-cost areas. For this reason, as well, the Commission has a "statutory responsibility to determine the likely economic consequences" of the proposed rule.[52]

---

[49] *See* Exec. Order No. 13,771, Reducing Regulation and Controlling Regulatory Costs, 82 Fed. Reg. 9,339 (Feb. 3, 2017).

[50] *Michigan v. EPA*, 135 S. Ct. 2699, 2707 (2015).

[51] *Compare id.* at 2607–08 (statute authorizing agency to promulgate "appropriate and necessary" regulations require agency to consider cost), *with* 47 U.S.C. § 201(b) ("The Commission may prescribe such rules and regulations as may be necessary in the public interest to carry out the provisions of this chapter."), *id.* § 254(b)(7) (authorizing the Commission to adopt universal service principles that "are necessary and appropriate for the protection of the public interest, convenience, and necessity and are consistent with this chapter"), *and id.* § 254(c)(1) (requiring the Commission to "establish periodically" a definition of universal service that is, *inter alia*, "consistent with the public interest, convenience, and necessity").

[52] *Bus. Roundtable v. SEC*, 647 F.3d 1144, 1148 (D.C. Cir. 2011).

The Commission must identify and weigh the costs and benefits of the proposed rule and furnish a reasoned analysis of why the benefits exceed the costs.[53] The agency must "quantify" the costs or "explain why those costs could not be quantified."[54] The agency's analysis also must "account[ ] for benefits as well as costs,"[55] but cannot engage in a "sham" exercise wherein the "'cost-benefit analysis' would always be tipped in favor of benefits."[56] "Simple logic, fairness, and the premises of cost-benefit analysis . . . demand that a cost-benefit analysis be carried out objectively."[57] In fact, Chairman Pai has long been a supporter of focusing on economics and championed the creation of the Office of Economics and Analytics, which is responsible for conducting cost-benefit analyses.[58] Unfortunately, the proposed rule imposes costs and detrimental impacts on carriers, consumers and markets and therefore the benefit of those actions could only be justified in the public interest if the reasons are unambiguous, convincing and actually promote nationwide solutions to the national security threat. It does not do this.

---

[53] *See Michigan*, 135 S. Ct. at 2707 ("Agencies have long treated cost as a centrally relevant factor when deciding whether to regulate. Consideration of cost reflects the understanding that reasonable regulation ordinarily requires paying attention to the advantages *and* the disadvantages of agency decisions.").

[54] *Bus. Roundtable*, 647 F.3d at 1149.

[55] *Pub. Citizen v. Fed. Motor Carrier Safety Admin.*, 374 F.3d 1209, 1222 (D.C. Cir. 2004).

[56] *Sierra Club v. Sigler*, 695 F.2d 957, 979 (5th Cir. 1983).

[57] *Id.*; *Bus. Roundtable*, 647 F.3d at 1148–49 (rule was arbitrary and capricious because SEC "inconsistently and opportunistically framed the costs and benefits of the rule").

[58] *See Establishment of the Office of Economics & Analytics*, MD Docket No. 18-3, Order, ¶¶ 3, 5 (rel. Jan. 31, 2018); 47 C.F.R. § 0.21(b)–(c), (e), (h), (j).

2. The proposed rule's immense costs will disproportionately harm small and mid-sized carriers that provide service in rural areas, including through roaming agreements with larger carriers.[59] The proposed rule will put some carriers out of business and disrupt the services provided by other carriers. Carriers will be unable to efficiently maintain and service the equipment they have in place. Outages will inevitably occur, both as a result of carriers shutting down and from the downtime necessary to replace equipment. Outages frustrate businesses, schools, and families in their everyday activities. They also endanger public safety; for example, people will be unable to call 911 or use their phones to get driving directions to the closest hospital. Moreover, consumers will be unable to update their devices' software. The inability to update software will prevent consumers from installing new security patches on their devices, increasing the risk of a breach. All of these harms will disproportionately fall on Americans living in rural areas—the regions of the nation that are least served by telecommunications and information services.

Moreover, the proposed rule will raise the cost of investing in replacement equipment. There is little certainty that a company that is approved today will not find itself targeted tomorrow; that uncertainty comes at a substantial cost to carriers deciding among vendors. And by pushing low-cost manufacturers and service-providers out of the market, the proposed rule will increase the price of other equipment and services, both because the lower end of the market has been chopped off, and because demand for the higher end of the market will increase without any assurance that existing manufacturers and service-providers can meet that demand with

---

[59] *See supra* Part II.

increased supply. Based on its members' experiences, CCA is particularly concerned that maintenance services will be inadequate, which will result in more frequent and longer outages.

The Commission recognized that thousands of small entities—carriers, healthcare providers, schools, and others—will be affected by the proposed rule.[60] But the Commission has not even attempted a preliminary estimate of the costs those small entities will shoulder if the proposed rule is adopted. In performing the analysis required by the Regulatory Flexibility Act, the FCC should carefully consider not just the direct impacts on small carriers, but also the trickle-down effects on other small entities in rural areas, including network outages and potential increases in carrier rates necessary to recoup a portion of the losses caused by the proposed rule. In light of these potentially crippling costs, the Commission has a further obligation "to minimize the significant economic impact" the proposed rule will impose on small entities, such as by adopting measures that might mitigate the harm the proposed rule will cause.[61]

3. In evaluating cost, the Commission also must take into account the carriers' substantial reliance interests. There can be no serious dispute that the proposed rule will "make[ ] worthless substantial past investment incurred in reliance upon" current law and Commission policy.[62] Although the Commission states that "the proposed rule would not apply to equipment already in place,"[63] the rule will destroy much or all of the value of that equipment. Networks that incorporate the targeted equipment will not last long without software and

---

[60] *See* NPRM, Appendix B ¶¶ 8–55.

[61] 5 U.S.C. § 604(a)(6); *see infra* Part VI.

[62] *Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 220 (1988) (Scalia, J., concurring).

[63] NPRM ¶ 18.

hardware upgrades and services. Even if the proposed rule does not expressly mandate that existing equipment be removed from the network, that is the rule's inevitable effect, because it prohibits the expenditure of USF funds on replacement equipment, upgrades, maintenance, service, and support provided by the targeted vendors.

In building their networks, carriers relied on the fact that this equipment was lawful. They did not have notice that the Commission would do an about-face and effectively outlaw this equipment. CCA is unaware of any instance where the Commission has banned USF recipients from purchasing products or services from a particular company, much less two of the market's largest vendors. On the contrary, the Commission ***encouraged*** carriers to provide low-cost access to telecommunications and information services, which incentivized the purchase, deployment, and use of cost-effective equipment, devices, and services.[64] Destroying reliance interests in this way—with no notice and no counterbalancing compensation—amounts to arbitrary agency action.[65]

The Commission's current USF policies do not discriminate against products sold by particular foreign companies. If the Commission now seeks to take a different approach, it "must be cognizant that longstanding policies may have 'engendered serious reliance interests that must be taken into account.'"[66] Where, as here, "decades of industry reliance on the

---

[64] Contributing to the problem, the FCC's reverse auction mechanism to distribute USF support encourages lowest priced bids and lower overall costs.

[65] *See Bell Atl. Tel. Cos. v. FCC*, 79 F.3d 1195, 1207 (D.C. Cir. 1996) (finding the rule in question valid because the "state of the law has never been clear" and regulated entities received "the benefit of their bargain").

[66] *Encino Motorcars, LLC v. Navarro*, 136 S. Ct. 2117, 2126 (2016) (quoting *FCC vs. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009)).

[Commission's] prior policy" is involved, it is particularly important to provide a fulsome explanation for why the agency is changing direction.[67]

4. The benefits of the proposed rule cannot sustain the immense costs the proposed rule will impose on smaller carriers and rural consumers. In fact, it is unclear from the NPRM exactly what benefits the Commission contemplates—a point that is underscored by the Commission's acknowledgment that it is not sure what benefits might flow from the rule, and how those benefits might be quantified.[68]

The Commission cannot rely on unspecified security concerns as a way of calculating benefits, but must "provide[ ] . . . evidence of a real problem" that the proposed rule will solve or mitigate.[69] The Commission cannot discharge this duty simply by citing a congressional report from 2012 that itself lacks any detail on the risks posed by targeted companies.[70] An agency's obligation to identify and calculate a rule's benefits applies with particular force where, as here, the benefits must be significant if they are to outweigh the rule's undeniably substantial costs. To "justif[y] such costly prophylactic rules," the agency "need[s] to explain how the potential danger" will be averted by the regulation.[71] The Commission has not done so here.

---

[67] *Id.* at 2126–27.

[68] *See* NPRM ¶ 33 ("Does this proposed rule improve our ability to safeguard the country's telecommunications networks from potential security risks? How can we quantify any such benefit to national security?").

[69] *Nat'l Fuel Gas Supply Corp. v. FERC*, 468 F.3d 831, 841 (D.C. Cir. 2006).

[70] *See* NPRM ¶¶ 4–5.

[71] *Nat'l Fuel Gas Supply Corp.*, 468 F.3d at 844.

B. The Proposed Rule Singles Out Smaller, Rural Carriers for Discriminatory Treatment, Contrary to the Very Purpose of the Universal Service Fund.

1. The proposed rule targets only one small portion of the sprawling and multifaceted American telecommunications network: carriers that receive USF funds. These carriers, who disproportionately serve rural areas, represent only one segment of the vast telecommunications and information services marketplaces. The proposed rule does not prevent networks operated by carriers covered by the proposed rule from interconnecting with networks operated by carriers that the rule does not cover and that may continue to use targeted equipment and services. Not only are some networks interconnected, but consumers may access non-covered networks through roaming agreements their carriers have with carriers whose networks are not directly affected by the proposed rule. And under the proposed rule, consumers will be allowed to purchase phones manufactured by targeted companies, so long as they do not buy them ***from*** carriers who receive USF money. The proposed rule thus harms the most vulnerable while doing little to address risks that may be posed by particular equipment, services, or devices in the rest of the country. An agency cannot ignore "an important aspect of the problem."[72] Indeed, "[s]uch an artificial narrowing of the scope of the regulatory problem," as the Commission proposes here, "is itself arbitrary and capricious."[73]

At a minimum, the Commission should address the use of USF funds to purchase certain equipment and services that may pose a national security risk only within the context of a comprehensive rulemaking that considers ***all*** telecommunications providers and ***all*** uses of the

---

[72] *Motor Vehicle Mfrs. Ass'n v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

[73] *Home Box Office, Inc. v. FCC*, 567 F.2d 9, 36 (D.C. Cir. 1977).

relevant equipment and services. The Commission has offered no reason to believe that the products and services in question are used only by USF recipients and their customers.

2. The proposed rule is directly contrary to the USF's very purpose: supporting carriers that provide service to rural and low-density regions of the country. Since its inception in 1934, the Commission has been tasked with "mak[ing] available, so far as possible, to all the people of the United States . . . a rapid, efficient, Nation-wide, and world-wide . . . communication service with adequate facilities at reasonable charges."[74] This ultimate policy objective—now known as "universal service"[75]—"has remained a consistent and fundamental goal for the FCC, even as the nature of that service and the regulatory means of achieving it have changed."[76]

Congress has determined that universal service, which means ***affordable*** access,[77] should be promoted through the USF. The USF is intended to ***assist*** carriers in providing "services for high-cost, hard-to-reach rural areas, as well as indigent households and local institutions like schools, hospitals, and libraries."[78] The USF supplies "financial support in providing those critical services."[79] The USF's purpose is to help smaller and often rural carriers shoulder the economic burden of building out networks to reach the underserved and to provide products and services at affordable prices.

---

[74] 47 U.S.C. § 151.

[75] *See id.* § 254

[76] *AT&T, Inc. v. FCC*, 886 F.3d 1236, 1241 (D.C. Cir. 2018).

[77] *See* 47 U.S.C. § 254(b)(1).

[78] *AT&T*, 886 F.3d at 1242.

[79] *Id.*

The proposed rule directly contradicts that purpose by imposing substantial costs on primarily rural carriers to the detriment of underserved populations. Moreover, the FCC's proposed rule could eliminate a substantial portion of the supplier market for core network equipment.[80] While there are a myriad of suppliers for discrete network components, a carrier's core network could likely be the most vulnerable to harmful attacks. As discussed above, the rule therefore conflicts with the Section 254(b) principles. For the same reasons, it violates the APA, as an agency action that "fail[s] to consider . . . a factor the agency must consider under its organic statute" is arbitrary and capricious.[81]

C. The Commission Has Not Identified Evidence Supporting Its Proposed Rule, Nor Has It Tailored the Rule to the Asserted Risk.

The Commission has failed to identify evidence supporting the broad prohibitions contemplated by the proposed rule. An agency must base its rules on the evidence before the agency and cannot rely on unsupported assumptions.[82] Indeed, agencies are obligated to demonstrate that their proposals are founded on and responsive to real problems. Here, the nature of the problems that the FCC is trying to address is not explained or established with evidence. To the contrary, the NPRM rests on premises that are ***not*** supported by any evidence identified by the Commission—and the Commission gives no reason for why the sweeping prohibitions it proposes are necessary in light of the dangers in question, or why its rule could

---

[80] The proposed rule will reduce the number of suppliers of core network equipment from five to three. There are additional providers of discrete network components.

[81] *Pub. Citizen*, 374 F.3d at 1216.

[82] *Motor Vehicle Mfrs. Ass'n*, 463 U.S. at 43.

not be more narrowly tailored.[83] This is not to minimize the seriousness or credibility of those federal agencies that may have identified concerns. But it does highlight that confidential, vague, and undifferentiated security concerns are not a sound foundation for transparent and robust agency action, which must provide notice of the basis for a rule and the opportunity to contest that basis.

The Commission has not explained why it proposes to target ***companies*** instead of ***products***, when it is the equipment and devices that allegedly create the security risk.[84] There are valid reasons to believe that not all Huawei and ZTE products and services create security risks. For example, one European country recently approved Huawei 5G base stations.[85] And it is hard to understand how many run-of-the-mill products and services, such as routine maintenance work on existing equipment, pose a significant security threat.

Although the Commission notes that actor-specific prohibitions in the context of sensitive government contracts and grants exist or are being actively considered,[86] it offers no explanation as to why the same risks are present in the context of ordinary consumer use. In fact, the Commission provides no evidence supporting its apparent belief that the targeted equipment or services cannot be used in a safe way. The FCC has asked "which components or services are

---

[83] *See Del. Dep't of Nat. Res. & Envtl. Control v. EPA*, 785 F.3d 1, 16–18 (D.C. Cir. 2015) (holding that an "overbroad" regulation was "not rational" where "reasonable alternatives" were not "address[ed]").

[84] *See* NPRM ¶ 15 (requesting comment on this issue).

[85] Juan Pedro Tomás, *Huawei gets approval to ship 5G base stations to the EU*, RCR Wireless News, https://www.rcrwireless.com/20180423/5g/huawei-gets-approval-ship-5g-base-stations-eu-tag23 (Apr. 23, 2018).

[86] *See* NPRM ¶¶ 6–7.

most prone to supply chain vulnerabilities" and whether "equipment can be certified not to present a supply chain risk," among many other questions.[87] But without an explanation of what that supply chain risk ***is***, it is difficult for stakeholders to address the Commission's questions. Nor has the Commission examined the different risk portfolios of software services and physical maintenance services. It is difficult for stakeholders to adequately comment on the myriad possible permutations of equipment and services—not to mention vendors—the Commission could cover in its rule without the agency identifying the specific security risks it is attempting to address.

The Commission identifies no evidence suggesting that networks owned by carriers receiving USF support pose a special or unique danger. Congress knows how to identify networks that require special rules. In the Spectrum Act, Congress prohibited recipients of grants allocated for the public safety broadband network from using those funds to pay anyone barred by a federal agency "from bidding on a contract, participating in an auction, or receiving a grant."[88] But Congress has been silent with respect to USF funds, and the Commission has pointed to no reason that rural carriers, hospitals, schools, or libraries are the focal point of the country's network vulnerabilities.

Essentially the entirety of the FCC's cited evidence consists of an October 2012 report by the House Permanent Select Committee on Intelligence ("HPSCI").[89] But the report cites no

---

[87] NPRM ¶ 15.

[88] 47 U.S.C. § 1404(a), (c); *id.* § 1426(e) (establishing the Network Construction Fund); *id.* § 1442 (establishing a state and local implementation grant program).

[89] Permanent Select Committee on Intelligence, U.S. House of Representatives, *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (Oct. 8, 2012) (cited in NPRM ¶ 4).

specific evidence that Huawei or ZTE equipment and services create cybersecurity risk. Nothing in the report explains specifically how those products and services are unsafe for use by American carriers. Furthermore, if Huawei and ZTE presented such a high level of danger in 2012, why is this report still the critical piece of evidence ***in 2018***? Carriers and other stakeholders cannot effectively evaluate and take actions to address cybersecurity threats, including risks in the supply chain, if they are kept in the dark. That is why HPSCI recommended that the intelligence community "should actively seek to keep cleared private sector actors as informed of the threat as possible" and that Congress should enact legislation aimed at "increasing information sharing among private sector entities."[90]

All indications suggest that the Commission is rushing to do something to address a problem that is little understood, or at least a problem that has not been explained to stakeholders and other members of the regulated public. As a result, it is unlikely that this NPRM will result in "a record enabling [a court] to see why the agency reacted to major issues of policy as it did."[91] Without a more focused inquiry and a presentation of evidence supporting the rulemaking, a court will be unable to "fathom how the Commission reached the conclusion that the balance here should be struck in favor of regulation."[92]

V. The Proposed Rule Is Unconstitutional.

The proposed rule raises serious constitutional questions by interfering with longstanding investment-backed expectations and depriving rural carriers of any economically beneficial use of their property. Absent a provision making these carriers whole for the devastating economic

---

[90] *Id.* vi–vii, 45–46.

[91] *Home Box Office*, 567 F.2d at 41 (internal quotation marks and alterations omitted).

[92] *Id.*

losses they will undeniably suffer, the proposed rule violates due process and amounts to an uncompensated regulatory taking.

A. The Proposed Rule Violates Due Process.

The Commission's proposed rule will violate carriers' due process rights in two ways. First, the rule will eviscerate carriers' longstanding investment-backed reliance interests.[93] When carriers made their investments over the past decade or more, they "did not have fair notice of what [would be] forbidden."[94] Indeed, many carriers have recently upgraded, or are continuing to transition, their networks to the newest available technologies. The rule will "deprive citizens of legitimate expectations and upset settled transactions."[95] Carriers did not "kn[o]w they were taking a risk in" entering contracts with foreign suppliers.[96] Rather, they believed they were following the USF's mandate to provide affordable telecommunications access to underserved communities. The proposed rule is unconstitutional because it unfairly interferes with carriers' legitimate expectations without sufficient justification. The Commission's rule narrowly targets USF recipients without providing any evidence that the problem is limited to that segment of the market or that the rule will make a material impact on the security of the telecommunications network as a whole.

Second, the proposed rule fails to provide an opportunity to review "the unclassified evidence on which the official actor relied," thereby violating the due process rights of

---

[93] *See supra* Part IV.A.3.

[94] *FCC v. Fox Television Stations, Inc.*, 567 U.S. 239, 254 (2012).

[95] *Gen. Motors Corp. v. Romein*, 503 U.S. 181, 191 (1992).

[96] *Id.* at 192.

equipment, device, and service providers, as well as the carriers who rely on them.[97] These stakeholders do not have a real "opportunity to rebut" the evidence regarding network security risks because essentially no evidence has been offered.[98] The Commission so far has relied primarily on a House committee report that is almost six years old and that does not provide specific evidence regarding alleged security risks of using suspect companies' equipment, devices, and services.[99] Failing to present directly affected entities with the evidence relied upon by the Commission will infringe the due process rights of those affected entities.

B. The Proposed Rule Results in Unconstitutional Regulatory Takings.

The proposed rule also will result in unconstitutional regulatory takings. Carriers will be unable to continue using their property because they will be prevented from upgrading or repairing their networks and their software components. By depriving carriers of the ability to obtain the products and services they need to continue using the equipment and devices they have already purchased, the proposed rule effectively "denies all economically beneficial or productive use" of their property.[100]

Similarly, the proposed rule extinguishes the expected value of already purchased equipment and of contracts that contemplate future transactions. Even a law "that substantially furthers important public policies may so frustrate distinct investment-backed expectations as to

---

[97] *Ralls Corp. v. Comm. on Foreign Inv. in the U.S.*, 758 F.3d 296, 319 (D.C. Cir. 2014).

[98] *Id.*

[99] *See* NPRM ¶ 4.

[100] *Lucas v. S.C. Coastal Council*, 505 U.S. 1003, 1015 (1992).

amount to a 'taking.'"[101] And if the "economic impact of the regulation on the claimant" is substantial and "the character of the governmental action" is direct, as opposed to generally applicable, the regulation is more likely to be a taking.[102] The Commission's ends may be laudatory, but that cannot salvage a regulation that frustrates significant investment-backed expectations and will cause devastating economic injury. Nor is the regulation "a general regulation" of the kind that often survive takings challenges.[103] Rather, this regulation targets specific entities: USF recipients who purchase equipment, devices, and services from companies deemed to pose a security risk. That the restriction on purchasing upgrades and services arose ***after*** carriers bought and installed their equipment and devices underscores that the proposed rule will result in unconstitutional regulatory takings.[104]

A well-established indicator of an unconstitutional taking is when the costs of a "public interest" regulation are concentrated on the property owner. Here, rural carriers will disproportionately bear the burden for the security of the entirety of the nation's telecommunications network. "The bedrock principle of the Takings Clause, whatever doctrinal form cases interpreting it may take, has been consistently reiterated by the Supreme Court. It is that the Takings Clause is 'designed to bar Government from forcing some people alone to bear

---

[101] *Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 127 (1978).

[102] *Connolly v. Pension Benefit Guar. Corp.*, 475 U.S. 211, 225 (1986) (quoting *Penn Central*, 438 U.S. at 124).

[103] *Dist. Intown Props. Ltd. P'ship v. Dist. of Columbia*, 198 F.3d 874, 883 (D.C. Cir. 1999).

[104] *Cf. Murr v. Wisconsin*, 137 S. Ct. 1933, 1944 (2017) ("a use restriction which is triggered only after[ ] . . . a change in ownership should also guide a court's assessment of reasonable private expectations").

public burdens which, in all fairness and justice, should be borne by the public as a whole.'"[105] Rural carriers whose businesses will be destroyed or severely burdened by the proposed rule will obviously not receive a "benefit . . . roughly commensurate with the burdens they [will be] forced to bear."[106] Without at the very least providing additional funding to compensate these carriers for the losses they will suffer, the proposed rule will run afoul of the Fifth Amendment.

VI. If the Commission Proceeds with a Rule, It Should Make Substantial Changes to Mitigate the Proposed Rule's Harmful Impact.

The proposed rule threatens USF-supported carriers with economic devastation and poses serious dangers to consumers and public safety. In the event the Commission intends to move forward with this rulemaking, which we urge it not to do, it should adopt common-sense provisions to mitigate those harms, including the following:

- Narrow the rule's scope. Limit the rule to particular types of equipment, devices, and/or services that, based on specific record evidence, present legitimate security risks that cannot be fixed through software patching or other mechanisms. Parents, subsidiaries, and affiliates of listed companies should not be automatically covered, but rather should be reviewed independently using the same criteria. The Commission also should make it very clear that the rule only applies to direct spending on prohibited equipment, devices, and/or services. If the rule extends to funding of projects and services that utilize targeted equipment, devices, or services,

---

[105] *Colo. Springs Prod. Credit Ass'n v. Farm Credit Admin.*, 967 F.2d 648, 654 (D.C. Cir. 1992) (quoting *Armstrong v. United States*, 364 U.S. 40, 49 (1960)).

[106] *Id.* at 655.

that would drastically increase the odds that any given carrier will have to rip and replace substantial portions of its network; that result would render meaningless the FCC's assurance that it seeks only to regulate on a "going forward" basis.[107]

- Adequate transitional funding. Provide additional USF or other funds to offset the costs of compliance, especially for rural carriers who lack ready access to cost-effective replacement equipment and reliable substitute services.[108]
- Sufficient compliance period. Provide a sufficient phase-in period and/or delayed compliance date. Small to mid-sized rural carriers could need 10 years to replace network equipment and ensure an orderly and smooth transition. And the longer the period carriers have to comply, the greater ability they have to spread out costs to try to lessen the proposed rule's crippling financial impact. The compliance date, therefore, should be ten years after adoption of a final rule. If the FCC can show that certain equipment or services pose a more immediate danger, or a relatively serious security risk, a tiered phase-in period would be appropriate. Use of USF funds for Tier 1 equipment or services (immediately dangerous) would be prohibited three years post-adoption; use of USF funds for Tier 2 equipment or services (security risk is serious, but not immediate) would be prohibited six years post-adoption; use of USF funds for Tier 3 equipment or services (security risk is documented, but not as serious) would be prohibited ten years post-adoption.

---

[107] NPRM ¶¶ 2, 13.

[108] *See AT&T*, 886 F.3d at 1251 (holding that "additional funding" created a "safety valve" that assured "the scheme will not, in practice, be 'unfair' to" adversely affected entities).

- Waivers. Create a robust and meaningful waiver process using the traditional "good cause" standard provided in 47 C.F.R. § 1.3.[109] Important considerations should include, without limitation: the applicant's financial situation; the availability and price of alternative sources of equipment, devices, or services; and any documented support (including certifications, if available) regarding the safety of particular equipment, devices, or services. The Wireless Bureau is in the best position to assess whether a USF recipient has provided adequate justification for a waiver. Denials of applications for waivers should be appealable within the Commission to ensure fair, thorough, and consistent consideration.
- Grandfather contracts. Grandfather existing contracts, including multiyear contracts and contracts for future upgrades and/or services. Without a provision allowing for upgrades to and services for existing equipment, carriers will be forced to rip and replace all equipment purchased from now-prohibited entities. Change-in-law provisions, if they exist, would not solve that problem.
- Grandfather existing equipment. Allow upgrades to and services for existing equipment, regardless of whether a contract for upgrades and/or services is currently in place. Carriers have made substantial investments in their networks, based on existing law and Commission policy. Prohibiting upgrades and services would be

---

[109] *See Vt. Pub. Serv. Bd. v. FCC*, 661 F.3d 54, 65 (D.C. Cir. 2011) (noting that a waiver "process is a 'sign of reasonableness,'" and "an effort by an agency 'to cabin'" the regulation's "'potential sweep'" (quoting *Nat. Res. Def. Council v. EPA*, 822 F.2d 104, 120 (D.C. Cir. 1987)); *Rural Cellular Ass'n v. FCC*, 588 F.3d 1095, 1104–05 (D.C. Cir. 2009) (assessing rule's fairness by looking to whether regulated parties had a meaningful opportunity "to obtain an exception").

unfairly retroactive and would destroy those reasonable investment-backed expectations.

- Grandfather devices. Grandfather already purchased consumer devices, such as phones and tablets, including software updates and other related services.

VII. The FCC Should Issue a Further NPRM with an Updated, More Detailed Proposed Rule.

Any final rule that results from the Commission's NPRM is likely to be far more elaborate than the proposed rule. But without a more detailed proposed rule, the affected parties will be deprived of the chance to provide input on the regulations that will have a substantial effect on their businesses, and the FCC will be deprived of input that would help tailor the rule to maximize the accomplishment of its goals and minimize the costs. Other governmental bodies also are studying vulnerabilities in our nation's telecommunications network supply chain. As noted above, for example, DHS is on track to issue a detailed report later this summer. The FCC's final rule likely will take into account developments such as the DHS report—potentially important evidence that stakeholders will not have had an opportunity to comment on in the context of the FCC's proposed rulemaking. Importantly, the FCC must engage in a more focused dialogue with national security expert agencies to effectively address communications supply chain concerns to attack the problem holistically.

If the Commission issues a final rule without first seeking additional comment to address these developments, it will violate the Administrative Procedure Act's notice-and-comment

requirements.[110] The logical-outgrowth doctrine has limits.[111] There is little indication here what a final rule might look like. The NPRM poses 50 more express questions (87) than there are words in the proposed rule (37). CCA has attempted to answer the Commission's questions to the best of its ability and to suggest options the Commission might consider. But because the Commission has not put forward "a concrete and focused" proposal, the Commission has failed "to make criticism or formulation of alternatives possible."[112] And without sufficient notice, the Commission is unlikely to meet "its obligation to make a record enabling [a reviewing court] to see why the agency reacted to major issues of policy as it did."[113]

---

[110] 5 U.S.C. § 553.

[111] *See, e.g.*, *Small Refiner Lead Phase-Down Task Force v. EPA*, 705 F.2d 506, 549 (D.C. Cir. 1983) ("This purported notice, however, is too general to be adequate. Agency notice must describe the range of alternatives being considered with reasonable specificity. Otherwise, interested parties will not know what to comment on, and notice will not lead to better-informed agency decisionmaking.").

[112] *Home Box Office*, 567 F.2d at 36.

[113] *Id.* at 41 (internal quotation marks and alterations omitted).

VIII. Conclusion.

The Commission's intentions are laudable. But the proposed rule is not a proper or effective means of furthering national security. The Commission should withdraw the proposed rule. At the very least, the Commission should substantially revise the proposed rule to mitigate the immense harms it will engender and request further comment on the revised proposal.

Respectfully submitted,

/s/ Steven K. Berry

Steven K. Berry
Rebecca Murphy Thompson
Courtney Neville
COMPETITIVE CARRIERS ASSOCIATION
601 New Jersey Avenue, NW, Suite 820
Washington, DC 20001
(202) 449-9866
www.ccamobile.org

Theodore B. Olson
Thomas H. Dupree Jr.
Andrew G.I. Kilberg
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, NW
Washington, DC 20036
(202) 955-8500
www.gibsondunn.com

June 1, 2018

<u>Exhibit 22-A</u>

Declaration of Steven K. Barry

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
	)	

DECLARATION OF STEVEN K. BERRY

I, Steven K. Berry, declare as follows:

1. My name is Steven K. Berry. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. I am the President and CEO of Competitive Carriers Association ("CCA"). Our organization represents nearly 100 wireless providers ranging in size from small, rural carriers to larger regional and national carriers. CCA's member carriers serve anywhere from fewer than 5,000 customers to millions of customers. CCA also represents associate members, including equipment manufacturers and other vendors and suppliers of products and services throughout the supply chain that feeds mobile communications. CCA has taken a leading role in supporting cybersecurity and network security initiatives in light of the pressing need to secure the United States' telecommunications networks against hostile foreign actors, and regularly expresses its support for protecting America's telecommunications supply chain to stakeholders, regulators, and legislators. CCA is a voting participant as an industry partner in the Department of Homeland Security's National Coordinating Center for Communications, which is tasked with monitoring and preventing harm to the country's telecommunications infrastructure.

3. I communicate regularly with CCA members about policy and legal developments that may affect the telecommunications market generally or their businesses directly. I work closely with my staff, which includes government relations, regulatory, and legal teams, to communicate our members' concerns and opinions to appropriate agencies, committees, legislators, and staff in Washington, D.C., and across the country. My staff also is in daily contact with our members on issues of vital importance to the business and regulatory environment affecting competitive carriers. I have testified numerous times before congressional committees on a variety of issues affecting competitive telecommunications carriers, and CCA regularly participates in rulemakings and other policy initiatives conducted by the Federal Communications Commission ("Commission" or "FCC") and other relevant agencies.

4. The FCC's proposed rule regarding national security threats to the communications supply chain is extremely important to CCA's members. My staff and I have spoken with dozens of our members about the proposed rule. It is far and away one of our members' most pressing concerns. I have personally discussed with carrier executives how the proposed rule would affect their businesses and, through my staff, have collected feedback from many more carriers. The statements below are based on those discussions and my decades representing the telecommunications industry, during which I have become very familiar with the marketplaces that would be affected by the proposed rule.

5. Rural carriers must contend with higher costs and larger and more sparsely populated geographic coverage areas. Equipment, devices, and services often are more expensive for rural carriers because needed supply is lower and the costs of deployment are higher and these carriers do not possess the scope or scale to always garner the attention of the largest manufacturers. These problems are compounded by the technological difficulty of

providing reliable service to a population that is highly dispersed, often across varying and rugged terrain that experiences weather extremes.

6. For several decades, the Universal Service Fund ("USF") has been an important part of maintaining the development, growth, and preservation of rural America's access to critically important telecommunications and information services. USF funds support telephone, SMS, and data services for millions of Americans living in rural and other high-cost areas. Connectivity in rural areas is beginning to catch up to the rest of the country because of the critical support provided by the USF. While some of CCA's wireless carrier members have almost fully transitioned to 4G for data, all are looking either to deploy 4G, testing and deploying 4G VoLTE if it is not already in place, and looking ahead to 5G. High-speed, reliable connectivity buttresses public safety and underpins economic growth in an era where the internet and, especially, mobile platforms are critical to reaching and interacting with a diverse customer base. Greater rural connectivity serves not just residents of those areas, but also visitors and others traversing rural carriers' coverage areas, who have access to these networks on account of roaming agreements between rural carriers and larger regional and national carriers. The majority of the carriers who have helped connect rural America to the rest of the country realistically could not have built out their networks without USF funding, and many would not be able to survive without that funding.

7. Many USF-funded carriers, including CCA members, have used equipment provided by companies that are targeted by the proposed rule to build their networks and continue to use those companies' products and services to maintain those networks. The equipment and consumer devices offered by targeted companies are often two or three times less expensive than market competitors. Moreover, purchasing equipment is just one step in building

and maintaining a network. The services provided by equipment vendors is critically important, and CCA members value responsive and cost-effective customer services. These services include pre-deployment testing of new equipment to ensure that it will meet expectations, installation of new towers and equipment, upgrades to existing equipment, repairs to existing equipment, and on-the-ground troubleshooting of issues as they arise. Both scheduled upgrades and unexpected equipment failures can cause temporary outages in wireless coverage. The timeliness and quality of service providers make a big difference in the length of outages and the probability that outages will recur.

8. The services provided by the targeted companies are almost always less expensive and can be more reliable than their market competitors. Some of the larger vendors have "most favored nation" clauses in their purchase contracts with carriers serving large urban areas. These clauses effectively prevent those vendors from offering discounted rates to rural carriers. And certain vendors simply prioritize larger carriers with more urban and suburban footprints. For example:

a. One CCA member experienced a network outage in 2017 that lasted more than a day because the vendor did not service the affected equipment quickly. This affected nearly 40,000 consumers in rural and remote portions of the western United States, who were unable to reach emergency services or loved ones.

9. The targeted companies also provide customer support for consumer devices. The software that runs on phones, tablets, and other devices—including both operating systems and apps—must be updated regularly. The existing software communicates through the network with a server and, when an update is released, notifies the consumer that the download is

available. And when the update is downloaded, it often runs through the network. Strategies for infiltrating and compromising personal devices is constantly evolving; without the ability to download security updates, devices become highly vulnerable. Moreover, software that cannot be updated eventually will not work at all, which means not only that apps stop functioning one by one, but also that the device itself eventually becomes unusable.

10. The Commission's proposed rule would dramatically affect the market for core network equipment and services, resulting in substantially higher costs for rural carriers. Rural carriers also will be barred from dealing with a significant number of service providers and sellers of consumer devices. When lower-cost providers are eliminated from this market, supply decreases without a corresponding decrease in demand. Costs of equipment, devices, and services would rise. Uncertainty regarding which vendors might be determined in the future to present security risks would result in higher costs now. Both higher costs and market uncertainty would increase the cost of borrowing. And all those costs would likely mean higher rates for consumers, which when combined with the need for new devices would cause consumers to leave their carriers. The loss of customers would in turn increase costs for the remaining customers.

11. Furthermore, the proposed rule, as a practical matter, would likely require many carriers to rip and replace equipment purchased from targeted companies. Network equipment needs regular servicing and technology upgrades to remain usable and prevent recurring outages. It is uncertain whether upgrades provided by different manufacturers, as well as transitioning equipment piece-by-piece as it ages out, is practicable. Interoperability concerns mean that carriers cannot know whether such a hodge-podge transition period would allow their networks to run at optimal efficiency and provide services to their customers at the quality level promised

and expected. In order to ensure interim and long-term network continuity and to stay competitive in the constantly evolving telecommunications market, many carriers will have little choice but to replace all existing equipment purchased from targeted companies as quickly as possible.

12. Rural carriers' capital investment in the next generation of technology has already been chilled. Capital investments by CCA's carrier members have declined substantially in the first quarter of 2018, in large part because of anticipated tighter restrictions on carriers' access to equipment and services provided by certain foreign companies.

13. Discussions with CCA's carrier members have confirmed that the proposed rule would be devastating to many of them. For example:

a. One carrier that has roughly 100,000 wireless broadband customers estimates that the purchase price of replacement equipment is in excess of $300 million, including approximately $75 million to replace the core, and an additional $60 million in installation costs. The downtime from installing new equipment would cause the company to forego at least $50 million in roaming fees. In total, the proposed rule would result in $410 million in direct, "rip and replace" costs, and at a minimum $4 million in additional annual servicing costs, which does not take into account the likely higher costs of any materials, upgrades and inferior equipment and customer service.

b. Another member began installation of a new base station in a small town with a population of 26, according to the 2010 census, but as a result of recent actions by the administration, the member's vendor company has declined to complete software updates or to transfer software licenses, and the member has been unable to turn on LTE service as a result. . The result is that the carrier has been unable to turn on LTE service.

That same CCA member has three more base stations, which were installed to bring wireless broadband services to areas where wireline service is insufficient, but work on those stations has halted because of the same licensing issue and reasonable worry that a penalty would be assessed.

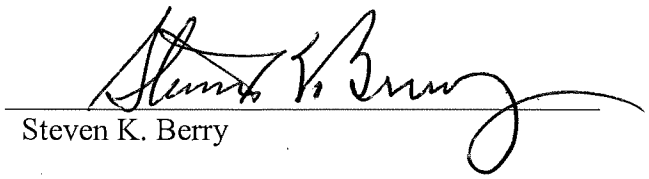
14. Lack of wireless coverage has real, tangible effects on rural Americans.

a. As another example, one CCA member serving portions of rural Nevada received local coverage as a result of its work to deploy a cell tower in Death Valley National Park in Nevada. As a result of this carrier's efforts, two French nationals, a 27-year-old man and a 21-year-old woman, were rescued from extreme heat after making a phone call that may not have connected before this cell tower was installed. Competitive carriers live and work in the communities they serve, as evidenced in Death Valley where service from a rural and regional provider offered the only area of coverage in a literal "dead" zone.

15. CCA's members, including regional carriers serving rural areas, care deeply about national security and are prepared to follow a coordinated process designed to enhance the security of our nation's communications networks. However, there is little, if any, material evidence of the benefits to our national security if the FCC adopts its proposed rule. Therefore, CCA is skeptical of an incomplete, uncoordinated approach that disproportionately penalizes small carriers and rural consumers without significant and immediate enhancements to the nation's national security. The FCC should defer to other expert agencies to address these concerns.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: June 1, 2018



Steven K. Berry

<u>Exhibit 22-B</u>

Declaration of Michael Beehn

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

DECLARATION OF MICHAEL BEEHN

I, Michael Beehn, declare as follows:

1. My name is Michael Beehn. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. I joined SI Wireless LLC d/b/a MobileNation ("SI Wireless") in 2018 as Chief Executive Officer. SI Wireless provides mobile phone and broadband services to approximately 20,000 customers across the western portions of Kentucky and Tennessee. We work to provide a reliable and more cost effective alternative to the larger nationwide wireless brands, and, as of today, SI Wireless is providing 4G service to approximately 80% of our predominantly rural customer base. Until the FCC released the proposed rule, we were actively engaged in strategic planning to provide 4G to the remaining 20% of our customers and defining our path to next-generation 5G services. If the FCC adopts its proposed rule or anything similar, it would be very difficult, if not impossible, for SI Wireless to maintain its current network and implement future network upgrades.

3. SI Wireless receives USF Lifeline support which enables us to offer discounted voice and mobile broadband service to nearly 4,000 low-income subscribers, representing about 20% of our customers.

4. Under its current business plans, SI Wireless has and, absent the FCC's proposed rule, planned to purchase equipment and services provided by a company the FCC appears to be targeting with its proposed rule. SI Wireless's core network infrastructure is constructed with and depends on Huawei equipment. SI Wireless chose Huawei because it delivered excellent quality and was the most cost-effective option for a rural network deployment. SI Wireless has been in business for approximately 8 years and in that time we have been impressed with the performance of Huawei equipment. Huawei also is our primary provider of on-the-ground customer services, such as installation of new and upgrade equipment, repairs of equipment, etc. Huawei is highly cost-effective and it provides excellent customer service.

5. The FCC's proposed rule threatens SI Wireless's ongoing viability. If the FCC's proposed rule is adopted, SI Wireless would have to replace all of its existing Huawei equipment, which represents a majority of its network. Although the proposed rule purports not to prevent SI Wireless from using equipment that it has already bought, it is unlikely that any other equipment manufacturer would be willing to economically work with Huawei to ensure interoperability if the rule was adopted, nor is it likely that we could, under the proposed rule, pay Huawei for those services. Prohibiting Huawei equipment and services would mean SI Wireless could not appropriately test and install new equipment to ensure it can work on SI Wireless's current network, thereby introducing the interoperability problems that we have until now avoided. To ensure that we can provide the service our customers expect, certain network equipment would have to be replaced. We estimate that the purchase price of replacement equipment is $40 to $60 million. That additional capital cost far exceeds what our EBITDA can financially support. This cost, in turn, would likewise force SI Wireless out of business and

leave thousands of subscribers in rural Tennessee and Kentucky with less competitive alternatives.

6. Customers would be severely affected. First, customers might lose coverage altogether and network outages would occur during equipment testing and installation. Second, our customers, especially low-income consumers on account of whom SI Wireless collects USF Lifeline support, could experience increased fees, or would lose service altogether, if the costs imposed by the proposed rule cannot be recouped through the USF or other sources of revenue. This will create a ripple effect resulting in further costs for SI Wireless by pushing customers to other carriers and critically diminishing our revenue.

7. If the proposed rule is adopted, SI Wireless will be faced with spending millions of dollars to comply with the proposed rule, if it can survive at all. The proposed rule threatens to destroy the business we've worked hard to build and to leave our customers without wireless service.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: June 1, 2018

Michael Beehn

<u>Exhibit 22-C</u>

Declaration of Frank Dirico

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
	)	

DECLARATION OF FRANK DIRICO

I, Frank DiRico, declare as follows:

1. My name is Frank DiRico. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. In 1991, I formed NE Colorado Cellular d/b/a Viaero Wireless ("Viaero") as the Founder, President and CEO. Viaero provides mobile telephone, SMS, and wireless broadband services to nearly 110,000 customers and approximately 1.5 million unique roaming customers per month across Eastern Colorado, Western Kansas, Nebraska and parts of Wyoming and South Dakota. We have worked aggressively to build out our network to include 2G/3G and 4G VoLTE. Until the FCC released the proposed rule, we were actively engaged in strategic planning, construction and equipment purchasing, including building a fiber network to our towers and to metropolitan areas in the continued effort to improve signal strength and speed to existing customers. Viaero's network has

been relied heavily on support from the Universal Service Fund ("USF"). USF funds are mission-critical to completing and maintaining Viaero's 4G VoLTE network and to the transition to 5G.

3. Viaero has purchased equipment and services from Huawei and would continue to do so if the FCC does not finalize its proposed rule. Viaero's network is made up largely of Huawei equipment. Approximately 80% of equipment, including core, wireless, microwave, and fiber, was manufactured by Huawei. Viaero chose Huawei because it was the most cost-effective option and the most reliable product and excellent customer service. Before contracting with Huawei, Viaero worked with a more expensive vendor whose product never was able to successfully deploy in our markets. Huawei's services have been much better, which has resulted in better network performance and less downtime. Viaero has consciously used a US-based vendor separate and distinct from Huawei for our firewalls, routers and switches. No traffic gets in or out of our network without going through our US-based vendors routers and firewalls. This gives Viaero protection from any malicious act by Huawei or anybody else. We have reached out to several cyber security firms to further evaluate any vulnerabilities in our network.

4. The FCC's proposed rule threatens Viaero's ability to survive. Viaero believes it will have to replace all of its existing Huawei equipment, which makes

up four-fifths its network. Although the proposed rule does not prevent Viaero from continuing to use equipment that has already installed, , we are very concerned that non-Huawei equipment will not be able to effectively interoperate with Huawei equipment and that other vendors will be able to adequately service Huawei equipment. We estimate that the purchase price of replacement equipment would be in excess of $300 million including approximately $75 million for to replace the core, and an additional $60 million in installation costs. During installation of the new equipment, Viaero will have to forego as much as $50 million in roaming fees from several national carriers. Viaero also would have to find a new service provider and initial estimates are approximately $4 million more annually than we currently pay. In total, the proposed rule would result in $410 million in direct, "rip and replace" costs, and $4 million in additional annual servicing costs, which does not take into account the likely higher costs of any materials, upgrades and lost time from installing inferior equipment and less responsive customer service from the other equipment manufacturers.

5. Our customers will be significantly impacted. Portions of the network will have to be taken down to test equipment before installation and during installation itself, most notably, 911 Phase 2 testing. Those outages will be significant. Customers will be unable to use their devices for everyday tasks, including contacting emergency services. These outages will affect not just Viaero's

subscribers, but also customers of other carriers that have roaming agreements with Viaero. Moreover, fees might have to be raised to recover some of the proposed rule's massive costs. We would expect a sizable loss of customers dissatisfied with higher fees and network downtime. Fewer customers means less revenue and greater difficulty maintaining, growing, and upgrading our network and services.

6. The uncertainty introduced by the FCC's proposed rule and other possible restrictions on using Huawei and ZTE equipment and services has been forced Viaero to reduce its capital investment in network capacity upgrades and expansion.

7. 7. The FCC's proposed rule would put Viaero in an almost impossible situation. We must decide whether to comply to the tune of $410 million in up-front costs, or not receive critical USF support. Regardless of which we choose, it will be a struggle to keep Viaero afloat. Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: June1, 2018

Frank DiRico

<u>Exhibit 22-D</u>

Declaration of James Groft

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
	)	

DECLARATION OF JAMES GROFT

I, James Groft, declare as follows:

1. My name is James Groft. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. In 2004, I was named CEO of James Valley Telecommunications (JVT) by the board of directors. JVT provides voice, mobile telephone, video, and broadband services to nearly 10,000 customers in South Dakota. We have worked aggressively to build out our 4G LTE network, and 100% of our predominantly rural customer base has full access to 4G LTE service. We have been actively engaged in strategic planning to be prepared for 5G. JVT's network has been built-out with support from the Universal Service Fund ("USF"). Without USF funds it would be impossible for JVT to make the transition to 5G and to maintain its 4G LTE network.

3. JVT has and, absent the proposed rule, would continue to purchase equipment, services, and devices provided by the companies the FCC appears to be targeting with its proposed rule. JVT's network is made up largely of Huawei equipment. 100% of our wireless core and wireless radios were manufactured by Huawei. JVT chose Huawei because it was the most cost-effective option with a 40% savings versus the 2nd most cost-effective option. Huawei

is also consequently our primary provider of customer support services, such as installation of new equipment and software upgrades. Huawei is highly cost-effective and it provides excellent customer service. Before contracting with Huawei, JVT had a series of terrible experiences with another, higher priced vendor. Huawei's service record, while not perfect, has resulted in fewer and less severe coverage outages for our customers. Huawei is there when our customers need them.

4. The FCC's proposed rule poses the single biggest threat to JVT's ongoing viability. JVT believes it will have to replace all of its existing Huawei equipment, which represents the lion's share of its network. Although the proposed rule does not prevent JVT from continuing to use equipment that it already purchased, we have very serious concerns about long-term interoperability if we were to continue using Huawei equipment in conjunction with newer equipment (including upgrades) from different manufacturers. A strict ban on using Huawei equipment moving forward would not allow JVT the time to properly test and calibrate new equipment to ensure it can work with a predominately Huawei legacy network. In order to ensure that we can provide the service our customers expect, we would have to make as clean a break as possible. We estimate that the purchase price of replacement equipment is close to $5,000 per affected customer and would result in the abandonment of a network that is not fully depreciated and does not need to be replaced.

5. Customer impact would be significant. Parts of our network will have to be shut down for significant periods of time to test equipment before installation and during installation itself. Consumers, including subscribers to other carriers who access our network pursuant to a roaming agreement between JVT and other carriers, will be unable to use their devices to call 911 or family members, process customer credit card payments, obtain driving directions, or

perform innumerable other tasks that rely on wireless connectivity. Unfortunately, our customers will certainly experience increased fees if the costs imposed by the proposed rule cannot be recouped through the USF or other sources of revenue. We would expect a measurable increase in customer's dissatisfaction because of higher bills and disruptions in coverage. This expected bump in customer dissatisfaction will create further costs for JVT by pushing customers to consider other carriers, which affects our revenue stream and exacerbates the problems directly engendered by the proposed rule.

6. Because of the uncertainty presented by the proposed rule and other possible governmental restrictions on Huawei JVT has restricted investment in its wireless network until the uncertainty has passed.

7. If the FCC adopts the proposed rule, JVT will be put between a rock and a hard place. Either JVT can forego USF funds, which are essential to our ability to maintain our existing network and to make the jump to 5G, or JVT can continue to accept USF funds and spend millions of dollars to comply with the proposed rule. Under either option, JVT's ability to survive would be put into serious question.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: May 29th, 2018

James Groft, CEO
James Valley Telecommunications

<u>Exhibit 22-E</u>

Declaration of Todd Houseman

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

DECLARATION OF TODD HOUSEMAN

I, Todd Houseman, declare as follows:

1. My name is Todd Houseman. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. In 2015, I joined United Telephone Association, Inc. ("United") as General Manager / CEO. I was named General Manager / CEO of United by the board of directors. United provides mobile telephone, SMS, and wireless broadband services to nearly 20,000 customers in 17 southwest Kansas counties. United was the first tier 3 wireless carrier in the United States to commercially launch a 4G LTE mobile network. That network covers United's entire licensed territory. United also provides wireline telephone service to 3,856 customers in 11 rural southwest Kansas exchanges and is currently deploying fiber-to-the-home in these communities.

3. The wireless network deployed by United consists primarily of Huawei equipment. Six years ago United chose Huawei due to two main factors. First, at the time, they were the only company manufacturing equipment that allowed United to fully utilize its spectrum holdings. The technical solution offered by Huawei was superior to other equipment manufacturers. Second, Huawei was by far the most cost effective.

4. The United networks (wireless, landline, and fiber) have been built with support from the Universal Service Fund ("USF") and United prides itself in being a good steward of these funds by deploying the most cost effective and technically sound networks possible. When the FCC released its proposed rule, United was in the process of ordering new Huawei equipment. This equipment would provide additional broadband internet speed to customers who do not live in or near a town by utilizing the recently purchased 600MHz spectrum. This project is now on hold. Without USF support United will not be able to build, operate, and maintain the new 600MHz wireless network.

5. United works hard every day to help further the FCC's goal to close the "digital divide" between urban and rural areas. Given the high cost to provide communication services in extremely rural areas United does rely on USF support. The uncertainty created by the proposed rule has forced United to freeze all capital investment in the 600MHz wireless network expansion and if adopted, would force United to scrap its existing plans and explore more costly alternative means of meeting the mandate to supply rural customers with broadband services.

6. United is a rural telephone cooperative in the heartland of America and nobody wants to protect our National Security more than United. But targeting certain equipment vendors, absent some means of certifying equipment from all manufacturers, injects an elevated level of risk for future network investment. Today the target is ZTE and Huawei; what assurance is there that other providers won't be the targets tomorrow?

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: June 1, 2018

Todd Houseman

<u>Exhibit 22-F</u>

Declaration of Michael D. Kilgore

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
	)	

DECLARATION OF MICHAEL D. KILGORE

I, Michael D. Kilgore, declare as follows:

1. My name is Michael D. Kilgore. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. In 2005, I joined Nemont Telephone Cooperative, Inc. ("Nemont") as Plant Operations Manager and, in 2009, I was promoted to General Manager and CEO of Nemont by the Board of Directors. Nemont provides mobile telephone, SMS, and wireless broadband services to nearly 12,000 customers across northeast and southcentral Montana, and northwest North Dakota through its wholly own subsidiary, Sagebrush Cellular, Inc. In many cases, Nemont's networks are the only networks in this service area. Not only do they serve their own customers, Nemont's wireless networks also serve nearly 300 million subscribers of the nation's largest carriers through roaming agreements. Nemont also provides wireline telephone and broadband access to approximately 20,000 customers in the States of Montana, North Dakota, and Wyoming. We have worked aggressively to build out our 4G network, and over 80% of our predominantly rural customer base has full access to 4G service. Until the FCC released the proposed rule, we were actively engaged in strategic planning to enhance our mobile broadband network. In building our network, we have relied on Universal Service Fund ("USF") support.

Continued USF support is essential for Nemont to enhance its 4G network, let alone make the transition to 5G.

3. Nemont's wireless network is made up largely of Huawei equipment; over 70%, including the core and RAN networks was manufactured by Huawei. Nemont selected Huawei as our wireless vendor due to its technical capabilities, customer support, and cost effectiveness. If the FCC adopts its proposed rule, Nemont believes it will have to replace all existing Huawei equipment as a result of the significant uncertainty regarding interoperability if Nemont could no longer contract with Huawei for services and replacement equipment. We estimate that the purchase price of replacement equipment is around $57 million including installation costs and the likely higher cost of any materials, support, and upgrades going forward. These costs threaten the viability of Nemont's wireless network.

4. Our customer base would be significantly impacted. Nemont's customers rely on our network to access emergency services, for business purposes, to learn, and to engage with the wider world. Customers likely would experience outages as we test and install replacement equipment. Additionally, customers might see higher bills because of the need to ameliorate the immense costs of network equipment replacement. Customer dissatisfaction would likely lead to decreased subscribership, which would further hit Nemont's bottom line.

5. Because of the uncertainty presented by the proposed rule and other possible governmental restrictions on Huawei, Nemont has significantly slowed down its capital investment in wireless network expansion. We have delayed our goal of 100% 4G coverage.

6. The FCC's proposed rule threatens to put Nemont out of the wireless business and leave its customers without wireless service. Regardless of whether Nemont chooses to go

without USF funds or to spend the tens of millions of dollars to comply with the new regulation, Nemont's viability would be put in jeopardy.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: June 1, 2018

Michael D. Kilgore

Michael D. Kilgore

Exhibit 22-G

Declaration of John C. Nettles

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
	)	

DECLARATION OF JOHN C. NETTLES

I, John C. Nettles, declare as follows:

1. My name is John C. Nettles. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. I am President and CEO of Pine Belt Cellular, Inc. ("Pine Belt") having served in that capacity since October 1994. Pine Belt provides mobile telephone, SMS, and wireless broadband services in the five Alabama counties of Choctaw, Dallas, Marengo, Perry and Wilcox.

3. Specifically, Pine Belt, along with its parent and affiliate companies, provides:

- 4G-LTE wireless broadband (both mobile and fixed), 3G-CDMA wireless broadband, 1xRTT wireless voice and broadband across the Alabama counties of Choctaw, Dallas, Marengo, Perry and Wilcox;
- ILEC and CLEC voice and broadband ILEC and CLEC services in parts of each county named above, plus Clarke County, Alabama; and
- Traditional HFC cable TV services in parts of Choctaw and Clarke Counties, Alabama.

4. The comments filed by the Competitive Carriers Association in the above-referenced docket are true and correct to the best of my knowledge. Pine Belt has also filed comments of its own, and it hereby refers to such comments for more information about its position on the matters presented in the above-referenced docket.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that, to the best of my knowledge, the foregoing is true and correct.

Executed on: June 1, 2018

John C. Nettles

<u>Exhibit 22-H</u>

Declaration of Eric J. Woody

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

DECLARATION OF ERIC J. WOODY

I, Eric J. Woody, declare as follows:

1. My name is Eric J. Woody. I am over the age of 18 and competent to make this declaration. The statements in this declaration are true and within my personal knowledge.

2. In 2008, I was promoted to Chief Technical and Operations Officer (CTOO) of Union Telephone Company d.b.a. Union Wireless ("Union") by the Union board of directors. Union provides mobile telephone, SMS, and wireless broadband services to nearly 40,000 customers across Wyoming, Colorado, Utah and Idaho. We have worked aggressively to build out our 4G LTE (Long Term Evolution) Data and 3G UMTS (Universal Mobile Telecommunication System) Voice network, and 90% of our predominantly rural customer base has full access to 4G LTE Data and 3G UMTS Voice service. Until the FCC released the proposed rule, we were actively engaged in strategic planning to be prepared for a complete overlay of 4G LTE with the introduction of VoLTE (Voice over LTE) by the end of 2018. We were also looking forward to performing 5G trials in early 2019 to get ready for the next evolution of technology in this industry. Union's network has been built-out with support from the Universal Service Fund ("USF"). Union receives approximately $20 million in USF funds

annually. Without USF funds, it would be very difficult, if not impossible, for Union to make the transition to 5G and to maintain its 4G VoLTE network.

3. Union has in the past and would continue to purchase Huawei equipment and services if the proposed rule is not adopted. Union's network is made up largely of Huawei equipment. Approximately 75% of Union's network equipment, including core, wireless, and microwave, was manufactured by Huawei. Union chose Huawei because it was the most cost-effective option as well as the only vendor who actually responded to my request for proposal at the time. It was necessary to change network vendors due to continued service interruptions, lack of timely support and excessive support costs. Again, Huawei is highly cost-effective and it has provided Union with excellent customer service. Before contracting with Huawei, Union had a series of terrible experiences with another, higher priced vendor. Huawei's service record has resulted in fewer and less severe coverage outages for our customers.

4. The FCC's proposed rule presents a singular threat to Union's ability to stay in business. Our past experience has shown us that other vendors cannot or will not interoperate with Huawei equipment. As such, the proposed rule would require Union to replace all the Huawei equipment in its network. We would have to install the new equipment and go through all the testing while operating dual parallel networks, then transition from the Huawei to the new vendor. We estimate that the purchase price of replacement equipment to be around $40 to $45 million, with approximately another $60 to $75 million in installation costs. We also estimate that it would take 5 years to completely transition from our Huawei network to a new vendor due to permitting and weather issues with being able to access to all of our facilities. The downtime from installing new equipment would cause Union to forego another $26 million in roaming fees annually from a larger carrier. Union also would have to find a new service provider; we

estimate our typical services will cost $2 million more annually than we currently spend. We also estimate a loss of approximately $20 million in lost USF annually while we continue to engage with Huawei during the transition process. In total, the proposed rule would result in $340 million in direct, "start-up" costs. This expense and activity would severely hamper our ability to further expand our service offering to areas with are currently underserved or unserved. Every dollar and hour spent of replacing equipment that would remain in place but for the FCC's rule is a dollar and hour not spent on expanding the network to reach those who desperately need these services.

5. Union's customers and roaming subscribers of other carriers who access our network pursuant to a roaming agreement between Union and those other carriers will be significantly impacted by the proposed rule. Even with dual parallel networks, outages could occur while equipment is tested and installed. This will also prevent all GSMA compliant devices from accessing 911/Emergency services during these outages. Other services that can be impacted include but are not limited to processing of customer credit card payments, obtain driving directions, or performing innumerable other tasks that rely on wireless connectivity. Customers might also end up with increased fees if additional revenue cannot be raised elsewhere. On account of all of this, it is likely that customer satisfaction and retention will decrease, which makes it even more difficult to sustain the business.

6. Union has halted some critical projects and significantly slowed down other capital investment in network expansion because of the uncertainty created by the proposed rule and other potential governmental actions related to Huawei. At this time of extreme uncertainty, we have tentatively pushed back our investment in IMS (IP Multimedia System) which is necessary for 4G VoLTE. It was out intention to be able to offer 4G VoLTE and VoWiFi (Voice

over WiFi) services throughout our LTE network by the end of 2018; now we will be lucky to be able to do it prior to the end of 2019 or possibly into 2020.

7. If the FCC adopts the proposed rule, Union will be put in a lose-lose situation. Union can stop taking USF funds, which are critical both to ongoing business and to transitioning to 5G. Alternatively, Union can shoulder more than $300 million to comply with the proposed rule and ensure ongoing USF support. Under either option, Union's ability to survive would be put into serious question. In the end the ones that suffer the most are those in current underserved and unserved areas that once again have to wait to get the services that the vast majority of others receive today; the customers in Rural America.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed on: June 1, 2018

_____

Eric J. Woody