

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
China Mobile International (USA) Inc.)	ITC-214-20110901-00289
)	
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

Adopted: May 9, 2019

Released: May 10, 2019

By the Commission: Chairman Pai and Commissioners O’Rielly, Carr, Rosenworcel and Starks issuing separate statements.

TABLE OF CONTENTS

Heading	Paragraph #
I. INTRODUCTION.....	1
II. BACKGROUND.....	2
A. International Section 214 Applications.....	2
B. China Mobile USA’s Application.....	3
III. DISCUSSION	8
A. Standard of Review.....	9
B. China Mobile USA is Vulnerable to Exploitation, Influence, and Control by the Chinese Government	14
C. Grant of the International Section 214 Authorization Would Produce Substantial and Serious National Security and Law Enforcement Risks	20
D. The National Security and Law Enforcement Risks Cannot be Addressed by Mitigation	34
IV. ORDERING CLAUSES.....	39
APPENDIX A –Classified Supplement	

I. INTRODUCTION

1. China Mobile International (USA) Inc. (China Mobile USA) is ultimately owned and controlled by the People’s Republic of China (Chinese government).¹ In this Memorandum Opinion and Order (Order), we deny China Mobile USA’s application for a section 214 authorization to provide

¹ Application of China Mobile International (USA) Inc. for International Section 214 Authority, File No. ITC-214-20110901-00289, Attach. 2 (filed Sept. 1, 2011), <https://go.usa.gov/xEhbs> (China Mobile USA Application); Amendment to Application of China Mobile International (USA) Inc. for International Section 214 Authority, File No. ITC-214-20110901-00289 (Jan. 30, 2015) (China Mobile USA 2015 Supplement).

international telecommunications services between the United States and foreign destinations.² After reviewing the record evidence in this proceeding,³ we find that due to a number of factors related to China Mobile USA's ownership and control by the Chinese government, grant of the application would raise substantial and serious national security and law enforcement risks that cannot be addressed through a mitigation agreement. Therefore, grant of this application would not be in the public interest.

II. BACKGROUND

A. International Section 214 Applications

2. Pursuant to section 214(a) of the Act, no carrier may provide service until it obtains from the Commission a certificate that such services will serve the public interest, convenience, and necessity.⁴ Section 63.18 of the Commission's rules, which implements section 214 of the Act, requires that an application for international section 214 authority "include information demonstrating how the grant of the application will serve the public interest, convenience, and necessity."⁵ As part of the Commission's public interest analysis, the Commission considers whether such an application raises national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's reportable foreign ownership.⁶ With regard to these concerns, the Commission has sought the expertise of the relevant Executive Branch agencies for over 20 years, and has accorded deference to their expertise when they have identified such a concern in a particular application.⁷ The Executive Branch agencies have provided

² China Mobile USA Application. Section 214 refers to section 214 of the Communications Act of 1934, as amended (the Act), 47 U.S.C. § 214.

³ We conclude that the publicly-available and business confidential information provided by the Executive Branch agencies, alone, is sufficient to support our findings and decision in this Order. In addition, there is a classified supplement that discusses how the classified information provided to the Commission by the Executive Branch agencies further supports the findings and decision in this Order. *See infra* Appendix A (Classified Supplement); 47 U.S.C. 154(j); *Use of Classified Information; Policy to be Followed in Future Licensing of Facilities for Overseas Communications*, Order, FCC 78-755, 44 Rad. Reg. 2d 607, 611, para. 10 (1978).

⁴ 47 U.S.C. § 214(a) ("No carrier shall undertake the construction of a new line or of an extension of any line, or shall acquire or operate any line, or extension thereof, or shall engage in transmission over or by means of such additional or extended line, unless and until there shall first have been obtained from the Commission a certificate that the present or future public convenience and necessity require or will require the construction, or operation, or construction and operation, of such additional or extended line. . . ."). The Supreme Court has determined that the Commission has considerable discretion in deciding how to make its section 214 public interest finding. *FCC v. RCA Communications, Inc.*, 346 U.S. 86, 90 (1953); *see also Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities Authorizations Therefor*, CC Docket No. 79-252, First Report and Order, 85 FCC 2d 1, paras. 117-29 (1980) (discussing the Commission's authority under section 214(a) of the Act); *Streamlining the International Section 214 Authorization Process and Tariff Requirements*, IB Docket No. 95-118, Notice of Proposed Rulemaking, 10 FCC Rcd 13477, 13480, para. 6 (1995); Report and Order, 11 FCC Rcd 12884, 12903, para. 44, n.63 (1996).

⁵ 47 CFR § 63.18.

⁶ *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market; Market Entry and Regulation of Foreign-Affiliated Entities*, IB Docket Nos. 97-142 and 95-22, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891, 23918-21, paras. 59-66 (1997) (*Foreign Participation Order*), recon. denied, 15 FCC Rcd 18158 (2000); *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, IB Docket No. 16-155, Notice of Proposed Rulemaking, 31 FCC Rcd 7456 (2016) (*Executive Branch Process Reform NPRM*).

⁷ *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66 (in opening the U.S. telecommunications markets to foreign entry, the Commission affirmed its previously *ad hoc* policy of seeking Executive Branch feedback on any national security, law enforcement, foreign policy, or trade policy concerns related to the reportable foreign ownership as part of its overall public interest review of an application). The policy also applies to other types of applications with reportable foreign ownership, including applications related to submarine cable landing

(continued....)

their advice on the record,⁸ and the Commission has considered their advice as a part of its public interest determination. The Commission ultimately makes an independent decision in light of the information in the record, including any information provided by the applicant in response to any filings by the Executive Branch agencies.⁹

B. China Mobile USA's Application

3. China Mobile USA is a Delaware corporation that is indirectly and ultimately owned and controlled by the Chinese government.¹⁰ China Mobile USA is an indirect but wholly owned subsidiary of China Mobile Limited, a Hong Kong entity that is publicly traded on the New York and Hong Kong exchanges.¹¹ China Mobile Limited is one of the largest telecommunications companies in the world.¹² China Mobile Hong Kong (BVI) Limited, a British Virgin Islands investment holding company, owns over 70% of China Mobile Limited.¹³ China Mobile Hong Kong (BVI) Limited is ultimately 100% owned by China Mobile Communications Corporation (China Mobile),¹⁴ which is 100% owned by the

(Continued from previous page) _____

licenses, transfers of control of domestic section 214 authority, and petitions for declaratory ruling to exceed the foreign ownership benchmarks of section 310(b) of the Act. *Id.*; *Amendment of the Commission's Regulatory Policies to Allow Non-U.S. Licensed Space Stations to Provide Domestic and International Satellite Service in the United States; Amendment of Section 25.131 of the Commission's Rules and Regulations to Eliminate the Licensing Requirement for Certain International Receive-Only Earth Stations*, IB Docket No. 96-111, CC Docket No. 93-23, RM-7931, Report and Order, 12 FCC Rcd 24094, 24171, paras. 179-80 (1997); *see also Executive Branch Process Reform NPRM*, 31 FCC Rcd at 7457-58, paras. 4-6.

⁸ *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66.

⁹ *Id.* (“We emphasize that the Commission will make an independent decision on applications to be considered and will evaluate concerns raised by the Executive Branch agencies in light of all the issues raised (*and comments in response*) in the context of a particular application.” (emphasis added)).

¹⁰ China Mobile USA Application and Attach. 2 and Exh. A; China Mobile USA 2015 Supplement at 2-3 and Revised Exh. A.

¹¹ China Mobile USA Application, Attach. 2; China Mobile USA 2015 Supplement at 2-3; *see also* China Mobile, *Overview*, <https://www.chinamobileltd.com/en/about/overview.php> (last visited Apr. 16, 2019) (China Mobile Limited was listed on the New York Stock Exchange on October 22, 1997 and the Hong Kong Stock Exchange on October 23, 1997).

¹² Through its subsidiaries, China Mobile is the dominant mobile provider in China and the world's largest mobile provider by subscribers. *See, e.g.,* Telegeography *China Mobile closing down 3G system, complete switch-off expected by 2020*, <https://www.telegeography.com/products/commsupdate/articles/2019/03/11/china-mobile-closing-down-3g-system-complete-switch-off-expected-by-2020/> (March 11, 2019). China Mobile Limited has the largest number of subscribers, with more than 925 million customers at the start of 2019, and a market value of \$217.5 billion in February 2019. The World's Top 10 Telecommunications Companies, <https://www.investopedia.com/articles/markets/030216/worlds-top-10-telecommunications-companies.asp> (Feb. 7, 2019).

¹³ China Mobile USA Application, Attach. 2 at 1 and Exh. A (74.2%); China Mobile USA 2015 Supplement at 2 and Revised Exh. A (73.31%). According to China Mobile's website, “[t]he Company's ultimate controlling shareholder is China Mobile Communications Group Co., Ltd. (formerly known as China Mobile Communications Corporation, “CMCC”), which, as of 31 December 2017, indirectly held approximately 72.72% of the total number of issued shares of the Company. The remaining approximately 27.28% was held by public investors.” China Mobile, *Overview*, <https://www.chinamobileltd.com/en/about/overview.php> (last visited Apr. 16, 2019).

¹⁴ According to its website, China Mobile Communications Corporation had a name change to China Mobile Communications Group Co., Ltd. China Mobile, *Overview*, <https://www.chinamobileltd.com/en/about/overview.php> (last visited Apr. 16, 2019); *see also* Bloomberg, *Company Overview of China Mobile Communications Group Co., Ltd.*, <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=7641651> (last visited Apr. 16, 2019).

(continued....)

Chinese government. China Mobile is a state-owned enterprise subject to the supervision of the State-Owned Assets Supervision and Administration Commission, a Chinese government body.¹⁵ China Mobile, through its subsidiaries, provides telecommunications services in China, Germany, Hong Kong, Japan, Pakistan, Singapore, and the United Kingdom.¹⁶

4. On September 1, 2011, China Mobile USA filed an application requesting authority under section 214 of the Act and section 63.18 of the Commission's rules to provide international facilities-based and resale telecommunications services.¹⁷ China Mobile USA plans to provide international telecommunications services to all international points (except those points on the Commission's exclusion list),¹⁸ including the destination countries in which it is affiliated with foreign carriers.¹⁹ China Mobile USA intends to offer international interexchange services and international private line circuits as well as mobile virtual network operator (MVNO) services.²⁰ China Mobile USA also plans to offer services that it states do not require an international section 214 authorization, such as data center and cloud services.²¹

5. On September 16, 2011, the Commission's International Bureau (Bureau) released a public notice finding China Mobile USA's international section 214 application acceptable for filing and placed the application on streamlined processing.²² Consistent with long-standing Commission policy and practice when reviewing the qualifications of applicants with reportable foreign ownership,²³ the

(Continued from previous page) _____

For ease of reference and to conform with the record, all references to China Mobile Communications Corporation are synonymous with China Mobile Communications Group Co., Ltd.

¹⁵ The State-Owned Assets Supervision and Administration Commission is directly under the management of the "State Council." Its responsibilities include supervising and managing the State-owned assets of centrally administered state-owned enterprises, appointment and removal of top executives of centrally administered state-owned enterprises, and the fundamental management of the State-owned assets of centrally administered state-owned enterprises. State-owned Assets Supervision and Administration Commission of the State Council, *What We Do* (July 17, 2018), http://en.sasac.gov.cn/2018/07/17/c_7.htm.

¹⁶ China Mobile USA Application, Attach. 1 and 2; China Mobile USA 2015 Supplement at 1-3.

¹⁷ China Mobile USA Application. China Mobile USA has stated that a more limited grant of resale-only authority would not be acceptable. Letter from Kent Bressie, Counsel to China Mobile International (USA) Inc., to Marlene H. Dortch, Secretary, FCC, File No. ITC-214-20110901-00289 at 1 (filed Oct. 6, 2014) (China Mobile USA Oct. 6, 2014 *Ex Parte* Letter); Letter from Kent Bressie, Counsel to China Mobile International (USA) Inc., to Marlene H. Dortch, Secretary, FCC, File No. ITC-214-20110901-00289 (filed Nov. 21, 2016) (China Mobile USA Nov. 21, 2016 *Ex Parte* Letter). On January 30, 2015, China Mobile USA filed updated ownership and foreign affiliate information. China Mobile USA 2015 Supplement.

¹⁸ FCC, *Exclusion List* (Nov. 17, 2015), <https://www.fcc.gov/general/exclusion-list>.

¹⁹ China Mobile USA Application, Attach. 1; China Mobile USA 2015 Supplement at 1.

²⁰ China Mobile USA Nov. 21, 2016 *Ex Parte* Letter at 2. The provision of some of these services may also include a domestic U.S. component. China Mobile USA does not need an international section 214 authorization to offer domestic MVNO services. It does need such authority to transport the communications it receives as an MVNO operator from the United States to foreign points.

²¹ *Id.*; see also Executive Branch Recommendation at 5.

²² *Streamlined International Applications Accepted for Filing; Section 214 Applications* (47 C.F.R. § 63.18); *Section 310(B)(4) Requests*, File No. ITC-214-20110901-00289, Public Notice, Report No. TEL-01519S, 2011 WL 4336771 (IB rel. Sept. 16, 2011).

²³ *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66 (where an international section 214 applicant has reportable foreign ownership, the Commission seeks the expert advice of the relevant Executive Branch agencies).

Bureau sought the advice of the relevant Executive Branch agencies²⁴ on whether the application raises any national security, law enforcement, foreign policy, or trade policy concerns. On September 30, 2011, at the request of the Executive Branch agencies, the Bureau removed China Mobile USA's application from streamlined processing.²⁵

6. On July 2, 2018, after a lengthy review of the application and consultation with the U.S. intelligence community,²⁶ the National Telecommunications Administration (NTIA) of the Department of Commerce filed a recommendation on behalf of the Executive Branch agencies requesting that the Commission deny China Mobile USA's application due to substantial national security and law enforcement risks that cannot be resolved through a voluntary mitigation agreement.²⁷ This is the first instance in which the Executive Branch agencies have recommended that the Commission deny an application due to national security and law enforcement concerns.²⁸

7. China Mobile USA, on August 20, 2018, filed its opposition to the Executive Branch Recommendation.²⁹ On September 19, 2018, NTIA filed a reply on behalf of the Executive Branch agencies.³⁰

III. DISCUSSION

8. We find that, based on the public record, China Mobile USA has not demonstrated that its application for international section 214 authority is in the public interest.³¹ We find that China Mobile

²⁴ The Department of Homeland Security; the Department of Justice, including the Federal Bureau of Investigation; the Department of Defense; the Department of State; the National Telecommunications and Information Administration (NTIA) of the Department of Commerce; the United States Trade Representative (USTR); and the Office of Science and Technology Policy (Executive Branch agencies or agencies).

²⁵ *Streamlined International Applications Accepted for Filing; Section 214 Applications* (47 C.F.R. § 63.18); *Section 310(B)(4) Requests*, File No. ITC-214-20110901-00289, Public Notice, Report No. TEL-01521S, 2011 WL 4559713 (IB rel. Sept. 30, 2011).

²⁶ Between the removal of the China Mobile USA application from streamlined processing in 2011 and June 2018, the Executive Branch agencies had extensive discussions with China Mobile USA about the national security and law enforcement concerns pertaining to China Mobile USA's request for international section 214 authority. Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, File No. ITC-214-20110901-00289 at 4 (filed July 2, 2018), <https://go.usa.gov/xEhZ7> (Executive Branch Recommendation or Recommendation); China Mobile International (USA) Inc., Opposition to Petition to Deny, File No. ITC-214-20110901-00289 at 4 (filed Aug. 20, 2018) (China Mobile USA Opposition or Opposition).

²⁷ Executive Branch Recommendation.

²⁸ The Executive Branch agencies explain that although they “strongly support[] the policy of the [Commission] to promote robust foreign participation in the U.S. telecommunications market,” they must take into account that “the deepening integration of the global telecommunications market has created risks and vulnerabilities in a sector replete with a broad range of malicious activities.” *Id.* at 2-3. Accordingly, the Recommendation balances “maintaining an open investment policy and protecting our national security and law enforcement requirements.” *Id.* at 3. In this case, that balancing led to the Executive Branch agencies' recommendation that the Commission deny the China Mobile USA application. *Id.* at 2-3.

²⁹ China Mobile USA Opposition; *see also* Letter from Kent Bressie, Counsel to China Mobile International (USA) Inc., to Marlene H. Dortch, Secretary, FCC, File No. ITC-214-20110901-00289 (filed May 1, 2019) (China Mobile USA May 1, 2019 *Ex Parte* Letter).

³⁰ Reply of the National Telecommunications and Information Administration, File No. ITC-214-20110901-00289 (filed Sept. 19, 2019) (Executive Branch Reply).

³¹ On February 11, 2013, Anthony J. Brindisi, Member, New York State Assembly, submitted a letter requesting that the Commission deny the China Mobile USA application. Letter from Anthony J. Brindisi, Member, New York

(continued....)

USA is vulnerable to exploitation, influence, and control by the Chinese government. We also find that, in the current security environment, there is a significant risk that the Chinese government would use the grant of such authority to China Mobile USA to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States. We find that those risks cannot be adequately addressed through a mitigation agreement. Thus, we deny China Mobile USA's application for international section 214 authority.

A. Standard of Review

9. Under section 63.18 of the Commission's rules, China Mobile USA must demonstrate how grant of its international section 214 application would serve the public interest, convenience, and necessity.³² In this section, we address China Mobile USA's argument that U.S. commitments under the World Trade Organization (WTO) and General Agreement on Trade in Services (GATS) establish a rebuttable presumption that grant is in the public interest. As discussed below, although an applicant with foreign ownership from a WTO Member country is entitled to a rebuttable presumption that grant is in the public interest on competition grounds, there are several other factors involved in our public interest review, including any national security and law enforcement issues. Such an applicant is not entitled to a rebuttable presumption with regard to these other factors.

10. China Mobile USA characterizes the Executive Branch agencies' submission as a petition to deny China Mobile USA's application and argues that the agencies have the burden of showing that grant of the application would be contrary to the public interest.³³ China Mobile USA asserts that the Commission does not require an applicant to prove by a preponderance of evidence that the public interest would be served, as this approach "would be inconsistent with the rebuttable presumption of market entry by foreign carriers from WTO member states."³⁴ The Executive Branch agencies reply that their Recommendation does not alter the threshold obligation of China Mobile USA to demonstrate that grant of the application is in the public interest under section 63.18 of the Commission's rules.³⁵ They assert that the burden of proof must stay with China Mobile USA.³⁶

(Continued from previous page) _____

State Assembly to Julius Genachowski, Chairman, FCC (filed Feb. 11, 2013) (Brindisi Letter). In reply, China Mobile USA urged the Commission to disregard the Brindisi Letter on both procedural and substantive grounds. Letter from Jennifer L. Kostyu, Counsel to China Mobile International (USA) Inc., to Marlene H. Dortch, Secretary, FCC, File No. ITC-214-20110901-00289 (filed March 12, 2013). China Mobile USA argued that Mr. Brindisi did not submit his letter during the relevant public notice period, did not serve it on China Mobile USA, and failed to include specific facts or evidence establishing that grant would be contrary to the public interest. *Id.* Because we deny the application in response to the national security and law enforcement considerations raised in the Executive Branch Recommendation, we do not separately address the merits of the *ex parte* filing.

³² 47 CFR § 63.18.

³³ China Mobile USA Opposition at 6 ("it is the Executive Branch that must make 'specific allegations of fact' as part of 'a prima facie showing that . . . a grant of the application would be inconsistent with the public interest, convenience and necessity'" (citing 47 CFR § 1.939(d)).

³⁴ *Id.* at 6. China Mobile USA states that in the *Foreign Participation Order*, the Commission adopted a rebuttable presumption that applications for international section 214 authority from carriers from WTO Member Countries, such as China, do not pose competitive concerns that would justify denial of the application. *Id.* at 5 (citing *Foreign Participation Order*, 12 FCC Rcd at 23913, para. 50); World Trade Organization, Members and Observers, https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm (last visited Apr. 16, 2019). China Mobile USA acknowledges that the *Foreign Participation Order* does not presume an application presents no national security, law enforcement, foreign policy, or trade policy concerns. China Mobile USA Opposition at 5.

³⁵ Executive Branch Reply at 6-7.

³⁶ *Id.* and n.23.

11. We conclude that China Mobile USA—the applicant for an international section 214 authorization—bears the burden of demonstrating that grant of its application would serve the public interest in accordance with section 63.18 of the Commission’s rules.³⁷ As set out in the Commission’s *Foreign Participation Order*, China Mobile USA is entitled to a rebuttable presumption that grant of its application would not be contrary to the public interest on competition grounds,³⁸ and nothing in this decision changes that. However, no such presumption applies to national security and law enforcement concerns, which are separate, independent factors the Commission considers in its public interest analysis.³⁹ As to those concerns, China Mobile USA has the burden to show that the public interest would be served by the grant despite the risks identified by the Executive Branch agencies.

12. China Mobile USA also asserts that the Commission’s review of its application should be informed by the WTO obligations of the United States.⁴⁰ In particular, it recognizes that U.S. commitments under the GATS do not prevent any Member country from taking any action it considers necessary for the protection of its “essential security interests,” but asserts that invocation of this exception requires notification to the WTO Council for Trade in Services.⁴¹ The Executive Branch agencies reply that nothing in the WTO or GATS prevents the Commission from soliciting or deferring to the Executive Branch agencies’ assessment of whether an application raises serious national security or law enforcement concerns.⁴² We agree. In adopting its *Foreign Participation Order* in 1997, the Commission addressed the referral of applications to the Executive Branch agencies for their advice and found that “taking these concerns into account is consistent with the GATS.”⁴³ U.S. obligations under the WTO and GATS do not prevent the Commission from seeking and considering the Executive Branch agencies’ assessment of national security and law enforcement risks.

13. China Mobile USA also argues that the Executive Branch review of the China Mobile USA application shows the lack of transparency and timeliness of the Executive Branch review process.⁴⁴ As China Mobile USA notes, the Commission has a pending proceeding to adopt rules related to the Executive Branch review process.⁴⁵ Issues and concerns about the review process are more appropriately addressed in that proceeding. China Mobile USA has had the opportunity in this proceeding to respond to

³⁷ 47 CFR § 63.18. As the Executive Branch agencies argue in their reply, section 63.18 requires an applicant to bear the burden of demonstrating that grant of its international section 214 application will serve the public interest, convenience, and necessity. Executive Branch Reply at 6 and n.21. The Commission ultimately makes an independent decision in light of the information in the record, including any information provided by the applicant in response to any filings by the Executive Branch agencies. *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66.

³⁸ *Foreign Participation Order*, 12 FCC Rcd 23891, 23920-21 para. 65 (“[W]e presume that an application from a WTO Member applicant does not pose a risk of anticompetitive harm that would justify denial. [footnote omitted]... We will continue to consider these concerns [*i.e.*, national security, law enforcement, foreign policy, or trade concerns] independent of our competition analysis.”).

³⁹ *Id.*

⁴⁰ China Mobile USA May 1, 2019 *Ex Parte* Letter at 2.

⁴¹ China Mobile USA Opposition at 6-8.

⁴² Executive Branch Reply at 7-8 (“The Executive Branch, however, has carefully considered U.S. obligations under GATS and the WTO and has concluded that nothing in those agreements prevents the Commission from soliciting, or deferring to, an Executive Branch assessment of whether a foreign-affiliated application raises serious national security or law enforcement related concerns.”).

⁴³ *Foreign Participation Order*, 12 FCC Rcd at 23920, para. 65.

⁴⁴ China Mobile USA Opposition at 16-18; *see also* China Mobile USA May 1, 2019 *Ex Parte* Letter at 1-3.

⁴⁵ *Id.* at 3-4 (citing *Executive Branch Process Reform NPRM*, 31 FCC Rcd 7456).

the Executive Branch Recommendation to the Commission, and as noted below has failed to address the substantial concerns raised in that filing.

B. China Mobile USA is Vulnerable to Exploitation, Influence, and Control by the Chinese Government

14. The Executive Branch agencies state that China Mobile USA, which is indirectly owned and controlled by the Chinese government, is vulnerable to its exploitation, influence, and control and that China Mobile USA would likely comply with espionage and intelligence requests made by the Chinese government.⁴⁶

15. The agencies note that although China Mobile USA has asserted that the State-Owned Assets Supervision and Administration Commission, the Chinese government agency that supervises and manages the government's state-owned assets, is not directly involved in China Mobile USA's management or operation, China Mobile USA does not deny that it is subject to its supervision.⁴⁷ The agencies further state that when they asked China Mobile USA to provide a legal opinion as to whether it would be subject to China's legal framework for surveillance, and whether China Mobile USA could challenge the Chinese government's surveillance requests, China Mobile USA **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.].⁴⁸

16. China Mobile USA acknowledges in its application that its indirect controlling parent, China Mobile, is 100% owned by the Chinese government, and that China Mobile is subject to the supervision of the State-Owned Assets Supervision and Administration Commission, a Chinese government body.⁴⁹ It asserts, however, that despite the ownership and supervision of its parent by the Chinese government, China Mobile USA itself should not be viewed as under its influence and control. China Mobile USA argues that, as a Delaware-incorporated, California-based U.S. business, it is immune from such influence and control. It contends that it would not be susceptible to requests or demands from a foreign government because it is "subject to U.S. law and would not be required, by virtue of its direct or indirect foreign ownership, to comply with foreign government requests relating to its operations within the United States."⁵⁰ The Executive Branch agencies reply that China Mobile USA's status as a Delaware-incorporated, California-based U.S. business does not diminish the national security and law enforcement risks associated with the indirect ownership and control of China Mobile USA by the Chinese government.⁵¹ The Executive Branch agencies also cite multiple instances in which a U.S.

⁴⁶ Executive Branch Recommendation at 7-8; Executive Branch Reply at 8-9. As part of their national security and law enforcement review, the agencies take into account a range of factors when evaluating an application for international section 214 authorization. The agencies have outlined these factors to China Mobile USA as part of their review of its application. Executive Branch Recommendation 6-7, n.23 (citing Exh. 9, May 14, 2015 Letter from U.S. Dep't of Justice to China Mobile USA). One of the factors is "whether the applicant is vulnerable to exploitation, influence, and control by other actors—including whether an applicant's foreign ownership could result in the control of U.S. telecommunications infrastructure or persons operating such infrastructure by a foreign government or an entity controlled by or acting on behalf of a foreign government." Executive Branch Recommendation at 7-8.

⁴⁷ Executive Branch Recommendation at 3 and n.10 (citing Exhs. 1 & 2, Nov. 3, 2011 response from China Mobile USA to Executive Branch agencies' October 5, 2011 questions).

⁴⁸ Executive Branch Reply at 14 and n.47 (citing Exh. 3, Dec. 2, 2016 email from Kent Bressie to Executive Branch agencies).

⁴⁹ China Mobile USA Application; China Mobile USA 2015 Supplement.

⁵⁰ China Mobile USA Opposition at 9.

⁵¹ Executive Branch Reply at 9-10.

subsidiary of a Chinese company owned and controlled by the Chinese government has invoked procedural and substantive bars to the service of legal process on the subsidiary in the United States, as highlighting the difficulties of serving process in the United States in order to enforce U.S. law on Chinese companies, including state-owned enterprises, operating within the United States.⁵²

17. The Executive Branch agencies' assessment that China Mobile USA is subject to influence and control by the Chinese government⁵³ is supported by our understanding that Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world.⁵⁴ For example, Article 7 of the 2017 National Intelligence Law provides that "[a]n organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows."⁵⁵ Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment.⁵⁶

18. Other analyses of Chinese state-owned enterprises by the U.S. government and by international organizations consistently have similarly found that state-owned enterprises are vulnerable to control by the Chinese government. For example, World Bank reports conclusively demonstrate that Chinese state-owned enterprises are not independent of the Chinese government despite more than two decades of reform, and that, historically, there has been little effective separation between the Chinese

⁵² *Id.* at 10-12.

⁵³ Executive Branch Recommendation at 7-8, 16; Executive Branch Reply at 8-9, 17.

⁵⁴ See, e.g., Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019 at 101 ("The 2017 *National Intelligence Law* requires Chinese companies . . . to support, provide assistance, and cooperate in China's national intelligence work, wherever they operate."); Ellen Nakashima, *Current, Former Pentagon Leaders Sound Alarm on Chinese Technology in 5G Networks*, THE WASHINGTON POST, Apr. 3, 2019, https://www.washingtonpost.com/world/national-security/current-former-pentagon-leaders-sound-alarm-on-chinese-technology-in-5g-networks/2019/04/02/d74f2bfe-54ab-11e9-9136-f8e636f1f6df_story.html?utm_term=.6002b02e8560 (attaching Statement by Former U.S. Military Leaders which states in part, "Espionage: Chinese-designed 5G networks will provide near-persistent data transfer back to China that the Chinese government could capture at will. This is not our opinion or even that of our intelligence community, but the directive of China's 2017 Intelligence Law, which legally requires that 'any organization or citizen shall support, assist, and cooperate with' the security services of China's One-Party State."); Remarks at Press Availability, Robert L. Strayer, Deputy Assistant Secretary for Cyber and International Communications and Information Policy (Feb. 26, 2019), <https://go.usa.gov/xEh9H> ("Chinese law requires [] firms to support and assist Beijing's vast security apparatus, without any democratic checks and balances on access to, or use of, data that touches the networks or equipment installed and supported by these companies around the world.").

⁵⁵ National Intelligence Law of the P.R.C. (2017), Article 7; see The National People's Congress of the People's Republic of China, *National Intelligence Law of the People's Republic*, http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm (last visited April 16, 2019). For an English-language translation, see, e.g., pkulaw.cn, *National Intelligence Law of the People's Republic of China (2018 Amendment)*, <http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law> (last visited April 16, 2019).

⁵⁶ Other Chinese laws obligate citizens and organizations to cooperate with intelligence activities. See, e.g., Lawfare, Beijing's New National Intelligence Law: From Defense to Offense (July 20, 2017), <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense> (citing the laws on Counterespionage (2014), National Security (2015), Counterterrorism (2015), Cybersecurity (2016), and Foreign NGO Management (2016), as well as the Ninth Amendment to the PRC Criminal Law (2015), the Management Methods for Lawyers and Law Firms (both 2016), and the pending draft Encryption Law and draft Standardization Law).

government and its state-owned enterprises.⁵⁷ The USTR, in its recently released 2018 Report to Congress on China's WTO Compliance, shares the World Bank's assessment that the Chinese government continues to exert control over Chinese state-owned enterprises.⁵⁸ The *2018 USTR WTO Report* catalogs the various mechanisms that the government and Communist Party use to control and influence the decisions of state-owned enterprises and states that some of the policies and practices mentioned in earlier World Bank reports are still in place. For example, the USTR states that the government and Communist Party appoint and control key executives through the Chinese Communist Party Organization Department.⁵⁹ Other policies and practices mentioned in the *2018 USTR WTO Report* demonstrate a concerted effort to further reinforce and expand government and Communist Party influence over state-owned enterprises. For example, the USTR notes that both state-owned enterprises and private Chinese companies are being pressured to amend their articles of association to ensure Communist Party representation on their boards of directors, usually as Chairman of the Board, and to ensure that they make important company decisions in consultation with internal Communist Party committees.⁶⁰ In addition, state-owned enterprises are still heavily subsidized, continue to enjoy preferential access to important inputs, such as land and capital, and still absorb a larger share of total credit than private Chinese companies.⁶¹

⁵⁷ International Bank for Reconstruction and Development, China's Management of Enterprise Assets: The State as Shareholder at vii-viii, 11, 14-15, 28 (1997), <http://documents.worldbank.org/curated/en/575461468769271136/pdf/multi-page.pdf> (1997 World Bank Report). For example, as state-owned enterprises were reorganized into modern corporations with boards of directors and some state-owned enterprises listed shares on China's nascent stock market, government and Communist Party (Party) officials preserved their control over the appointment and dismissal of many key managers, and government or Party bodies also nominated the members of boards of directors. 1997 World Bank Report at ix, 15; see also Stoyan Teney and Chunlin Zhang, *Corporate Governance and Enterprise Reform in China: Building the Institutions of Modern Markets* (2002), <http://documents.worldbank.org/curated/en/684341468241203489/pdf/multi0page.pdf>. In addition, while the establishment of China's State-Owned Assets Supervision and Administration Commission in 2003 represented a major step forward in China's state-owned enterprise reform, there has been a tendency for the State-Owned Assets Supervision and Administration Commission to become increasingly involved in the business operation of state-owned enterprises. Chunlin Zhang, *The World Bank in China's State-Owned Enterprise Reform Since the 1980s* at 7 (2019), <http://documents.worldbank.org/curated/en/828251550586271970/pdf/134778-World-Bank-in-China-SOE-reform-final-Feb-09-2019-En.pdf> (2019 World Bank Report). The State-Owned Assets Supervision and Administration Commission was established at the World Bank's recommendation to centralize China's management of state enterprise assets by creating a single government agency that specializes in exercising state ownership rights. 2019 World Bank Report at 5-7.

⁵⁸ USTR, 2018 Report to Congress on China's WTO Compliance (Feb. 2019), <https://go.usa.gov/xmB86> (2018 USTR WTO Report).

⁵⁹ *Id.* at 12.

⁶⁰ *Id.* at 13. Furthermore, the Communist Party has endorsed the Social Credit System, which is expected to be fully operational in the year 2020. *Id.* The Social Credit System will be used by the government "to monitor, rate and condition not only the conduct of all individuals in China, but also all domestic and foreign companies in China" and "it appears that the government will use the Social Credit System, among other things, to ensure that economic actors follow industrial plans." *Id.* In addition, the 2018 USTR WTO Report notes that legal institutions, including the courts, are structured to respond to the Party's direction and "to the extent that companies and individuals seek to act independently of government or Party direction, the legal system does not provide a venue for them to achieve these objectives on a systemic or consistent basis." *Id.* at 14.

⁶¹ *Id.* at 9, 12, 75-79. An example of government control discussed in the 2018 USTR WTO Report is a plan for classifying and evaluating the performance of state-owned enterprises that was jointly released by the State-Owned Assets Supervision and Administration Commission and China's Ministry of Finance in September 2016. Although commercially driven state-owned enterprises are expected to focus on earning reasonable returns on capital, the measure explicitly provides that their returns will be considered satisfactory if, for example, these enterprises are

(continued....)

19. In sum, we find China Mobile USA's argument that it is not susceptible to exploitation, influence, and control by the Chinese government because it is incorporated and based in the United States to be unpersuasive. The record does not provide any basis for the contention that China Mobile would not be treated similarly to other Chinese state-owned enterprises or that China Mobile USA itself, as a subsidiary of China Mobile, would not be subject to such control. Indeed, there is substantial risk that the Chinese government would exert even greater control over China Mobile and China Mobile USA than over other state-owned enterprises given the Chinese government's 100% ownership of China Mobile, the size and reach of China Mobile and its subsidiaries, and the importance of and opportunities afforded by the telecommunications services offered both within China and globally.⁶² In light of these findings, we conclude that China Mobile USA would, if granted the authority it seeks, be highly likely to succumb to exploitation, influence, and control by the Chinese government.

C. Grant of the International Section 214 Authorization Would Produce Substantial and Serious National Security and Law Enforcement Risks

20. Each international section 214 application requires an examination of the current national security environment with respect to a particular foreign government's activities, the link between those government activities and the security and integrity of telecommunications networks, and whether the activities raise national security concerns. We acknowledge that foreign government control of a U.S. carrier in and of itself is not grounds for denial of an international section 214 application. In fact, in keeping with the WTO commitments of the United States,⁶³ the Commission has granted several such

(Continued from previous page)

required to safeguard national security, among other circumstances involving their participation in the implementation of specified government policies and programs. *Id.* at 102.

⁶² China Mobile, through its subsidiaries, provides telecommunications services in China, Germany, Hong Kong, Japan, Pakistan, Singapore, and the United Kingdom. *See supra* at para. 3. Through its subsidiaries, China Mobile is the dominant mobile provider in China and the world's largest mobile provider by subscribers. *See, e.g.,* Telegeography *China Mobile closing down 3G system, complete switch-off expected by 2020*, <https://www.telegeography.com/products/commsupdate/articles/2019/03/11/china-mobile-closing-down-3g-system-complete-switch-off-expected-by-2020/> (March 11, 2019); David W. Barden, *Global Wireless Matrix: Emerging Market Revenue Growth Loses Steam; While Developed Markets Heading Positive*, *Industry Overview*, Bank of America Merrill Lynch, at 64, Tbl. 36: China Mobile (Oct. 3, 2018); Telegeography, *China Mobile H1 profit grows 4.7% as subscriber base passes 900m*, <https://www.telegeography.com/products/commsupdate/articles/2018/08/10/china-mobile-h1-profit-grows-4-7-as-subscriber-base-passes-900m/> (Aug. 10, 2018).

⁶³ The results of the WTO basic telecommunications services negotiation are incorporated into the GATS by the Fourth Protocol to the GATS, April 30, 1996, 36 I.L.M. 366 (1997). These results, as well as the basic obligations contained in the GATS, are referred to as the "WTO Basic Telecom Agreement." The WTO Basic Telecom Agreement advances the principles of open markets, private investment and competition, as well as the adoption of procompetitive regulatory principles. Under the terms of the Agreement, the United States has committed to allow foreign suppliers to provide a broad range of basic telecommunications services in the United States. Many countries, including the United States, also undertook additional specific commitments as a result of the negotiations in accordance with Article XVIII of the GATS. These additional commitments are the procompetitive regulatory principles contained in a document known as the "Reference Paper." The Reference Paper contains principles relating to competition safeguards, interconnection, universal service, transparency of licensing criteria, independence of the regulator, and allocation of scarce resources. *See* World Trade Organization, *Telecommunications Services: Reference Paper*, Negotiating Group on Basic Telecommunications (April 24, 1996), https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel23_e.htm. In the *Foreign Participation Order*, the Commission adopted an open entry standard for applicants from WTO Member countries, finding that an increasingly competitive environment and improved regulatory tools enabled the Commission to adopt a deregulatory approach that presumes foreign entry is in the public interest. *See generally Foreign Participation Order*. Still, as noted above, nothing in the GATS prevents the Commission from seeking and considering the Executive Branch agencies' assessment of national security and law enforcement risks. *See also Foreign*

(continued....)

authorizations to entities with foreign government ownership.⁶⁴ However, in this case, the Executive Branch agencies identify significantly enhanced national security and law enforcement risks linked to the Chinese government's activities since the Commission last granted international section 214 authorizations to other Chinese state-owned companies more than a decade ago.⁶⁵ The changes include the sophistication and resulting damage of the Chinese government's involvement in computer intrusions and attacks against the United States.⁶⁶

21. The agencies state that these developments support the Executive Branch agencies' current security assessment. They explain that prior Chinese government involvement in computer intrusions and attacks and economic espionage is one of the factors that gives rise to their assessment that grant of the China Mobile USA application would produce substantial and unacceptable national security and law enforcement risks.⁶⁷ The Executive Branch Recommendation cites press releases and other documents as well as numerous Congressional reports.⁶⁸

22. As a consequence, the agencies assess that the risks associated with granting an international section 214 authorization to China Mobile USA are now different and heightened, and raise

(Continued from previous page) _____

Participation Order, 12 FCC Rcd at 24049, para. 365 (“[o]n its face, GATS Article XIV bis allows measures to protect essential security interests”).

⁶⁴ See, e.g., *International Authorizations Granted, Section 214 Applications* (47 C.F.R. § 63.18, Section 310(B)(4) Requests, File No. ITC-214-20140918-00265, Public Notice, Report No. TEL-01828, 31 FCC Rcd 13418 (IB Dec. 22, 2016) (grant to Telekomunikasi Indonesia International (USA) Inc., whose parent entity is the Indonesian-government majority-owned incumbent telecommunications provider in Indonesia); *T.A. Resources N.V., Application for International Section 214 Authorization and Determination that Aruba Provides Effective Competitive Opportunities to U.S. Carriers*, IB Docket No. 10-228, File No. ITC-204-20100107-00010, Order and Authorization, 26 FCC Rcd 15978 (IB 2011) (grant to T.A. Resources N.V., a wholly-owned subsidiary of SETAR N.V., which, in turn, is wholly-owned by the government of Aruba); *International Authorizations Granted, Section 214 Applications* (47 C.F.R. § 63.18), Section 310(B)(4) Requests, File No. ITC-214-20081008-00453, Public Notice, Report No. TEL-01470, 25 FCC Rcd 17052 (IB Dec. 7, 2010) (grant to Office des Postes et Telecommunications de Polynesie Francaise, wholly owned by the government of French Polynesia).

⁶⁵ Executive Branch Recommendation at 14.

⁶⁶ *Id.*

⁶⁷ *Id.* at 8-14.

⁶⁸ *Id.* at 9 (citing Press Release, Office of Public Affairs, U.S. Dep't of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information (Mar. 23, 2016), available at <https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive>; see also Press Release, Office of Public Affairs, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), available at <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>; U.S.-China Econ. and Sec. Review Comm'n, *2014 Report to Congress of the U.S.-China Economic and Security Review Commission* (2014), available at https://www.uscc.gov/Annual_Reports/2014-annual-report-congress; U.S. Dep't of Def., *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China* (2013), available at http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf; Comm'n on the Theft of Am. Intellectual Prop., *The Report of the Commission on the Theft of American Intellectual Property* (May 2013), available at http://www.ipcommission.org/report/ip_commission_report_052213.pdf (IP Commission Report); Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (2013), available at <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> (Mandiant Report); H.R. Permanent Select Comm. on Intelligence, 112th Cong., *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (2012) (*House Report*), available at [https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20\(final\).pdf](https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf)).

special concerns due to the size and technical and financial resources of China Mobile USA's parent company and its subsidiaries.⁶⁹ Based on their knowledge of the risks of granting international section 214 authorizations to Chinese state-owned carriers, and in light of China's role in economic and other kinds of espionage against the United States,⁷⁰ they have concluded that prior mitigation measures applied to certain Chinese state-owned telecommunications companies operating in the United States would be insufficient here to address the risks posed by granting an international section 214 authorization to China Mobile USA.

23. China Mobile USA does not dispute or take issue with the Executive Branch agencies' statements that the Chinese government has taken actions against the interests of the United States.⁷¹ China Mobile USA argues, however, that the reports and other evidence provided in the Executive Branch Recommendation do not specifically pertain to China Mobile USA.⁷² For example, China Mobile USA argues that the Executive Branch agencies rely heavily on a 2012 House Report regarding security issues posed by Huawei Technologies Co. Ltd. (Huawei) and ZTE Corporation (ZTE), which does not mention China Mobile USA or its parent entities.⁷³

24. The Executive Branch agencies acknowledge that the reports cited in the Executive Branch Recommendation do not specifically mention China Mobile USA (which currently holds no Commission authorizations), but assert that the reports highlight concerns with actions by the Chinese government and Chinese state-owned enterprises.⁷⁴ They state that, "the Chinese government's policy of intertwining Chinese state-owned enterprise resources with intellectual property theft and economic espionage, along with the Chinese government's ongoing intelligence activities targeting the United States, presents too great of a risk in light of the fact that 'China Mobile Communications Company—and by extension, its subsidiary [China Mobile USA]—as a prominent Chinese [state-owned enterprise], cannot be expected to act against the interest of the Chinese government on any sensitive manner.'"⁷⁵ They cite, as an example, the *USTR Section 301 Report* that sets forth the Chinese government's "military-civil fusion" policy of "integrating platforms for information sharing between, among others, the People's Liberation Army (PLA) and Chinese enterprises in order to provide competitive intelligence to Chinese state-owned enterprises through the use of cyber intrusions."⁷⁶ They also cite the *Mandiant*

⁶⁹ Executive Branch Recommendation at 8.

⁷⁰ *Id.* at 8-14.

⁷¹ China Mobile USA Opposition at 8 (stating that China Mobile USA cannot and does not take issue with those concerns).

⁷² *Id.* at 10-13; *see also* China Mobile USA May 1, 2019 *Ex Parte* Letter at 2. China Mobile USA observes that in addition to the public filing, the Executive Branch agencies provided classified materials to the Commission. China Mobile USA requests that the Commission examine those classified materials to see if they relate to China Mobile USA specifically. *Id.* at 15-16; *see also* China Mobile USA May 1, 2019 *Ex Parte* Letter at 2.

⁷³ *Id.* at 10-13. China Mobile USA notes that it has no common ownership, governance, management, operation, or other coordination arrangements with either Huawei or ZTE, and that it has already voluntarily removed Huawei equipment from its U.S. network and has committed to not use Huawei equipment in its U.S. operations in the future. *Id.* at 11-13.

⁷⁴ Executive Branch Reply at 15.

⁷⁵ *Id.* at 13 and n.44 (quoting Executive Branch Recommendation at 8-9).

⁷⁶ *Id.* at 13-14 and n.45 (citing Office of U.S. Trade Rep., *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, at 170 (Mar. 22, 2018) (*USTR Section 301 Report*) (stating that "the U.S. government has evidence that the Chinese government provides competitive intelligence through cyber intrusions to Chinese state-owned enterprises through a process that includes a formal request and feedback loop, as well as a mechanism for information exchange via a classified communication system."); *see also* Office of U.S. Trade Rep., *2019 Special*

(continued....)

Report that states “the PLA’s cyber command is fully institutionalized within the CPC [Communist Party of China] and able to draw upon the resources of China’s state-owned enterprises to support its operations.”⁷⁷ Thus, according to the Executive Branch agencies, each of the national security and law enforcement concerns raised about the Chinese government also applies to China Mobile USA.⁷⁸

25. Due to these concerns, the agencies assert that grant of the China Mobile USA application would not be in the public interest in the current national security environment because it would produce substantial and unacceptable national security and law enforcement risks and these risks likely would increase over time.⁷⁹

26. In assessing the national security and law enforcement risks presented by an application, the Executive Branch agencies consider a range of factors including “[w]hether the applicant’s planned operations within the United States provide opportunities for an applicant or other actors to (1) undermine the reliability and stability of the domestic communications infrastructure, (2) identify and expose national security vulnerabilities, (3) render the domestic communications infrastructure otherwise vulnerable to exploitation, manipulation, attack, sabotage, or covert monitoring, (4) engage in economic espionage activities against corporations that depend on the security and reliability of the U.S. communications infrastructure to engage in lawful business activities, or (5) otherwise engage in activities with potential national security implications.”⁸⁰

27. The Executive Branch agencies state that if China Mobile USA is granted an international section 214 authorization, it would be able, as a common carrier, to connect to the network in the United States and would have greater access to the telephone lines, fiber-optic cables, cellular networks, and communication satellites that make up the network than an entity that does not have an international section 214 authorization.⁸¹ The agencies are concerned that an entity with such network access has the ability to target, alter, block, and re-route traffic.⁸² Based on the Executive Branch agencies’ experience and expertise in monitoring the security of network facilities, their need to work with service providers to identify and disrupt unlawful activities such as computer intrusions, and their need for assistance from trusted service providers when investigating past and current unlawful conduct,

(Continued from previous page)

301 *Report*, at 47 (Apr. 25, 2019) (“Since enacting its Cybersecurity Law [] in 2017, China has taken multiple steps backward through its efforts to invoke cybersecurity as a pretext to force U.S. [intellectual property]-intensive industries to disclose sensitive [intellectual property] to the government, transfer it to a Chinese entity, or both.”).

⁷⁷ Executive Branch Reply at 14 and n.46 (citing *Mandiant Report* at 7).

⁷⁸ *Id.* at 13-15.

⁷⁹ Executive Branch Recommendation at 7-14.

⁸⁰ *Id.* at 6; *see also* Exh. 9, May 14, 2015 Letter from U.S. Dep’t of Justice to China Mobile USA.

⁸¹ Executive Branch Recommendation at 10.

⁸² *Id.* Over the past year, various articles report that Chinese entities, including China Telecom, have been responsible for various Border Gateway Protocol (BGP) hijackings of U.S. traffic. *See, e.g.,* Chris C. Demchak and Yuval Shavitt, *China’s Maxim—Leave No Access Point Unexploited: The Hidden Story of China Telecom’s BGP Hijacking*, Vol. 3: Iss. 1, Article 7 Military Cyber Affairs (2018), <https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca>; Justin Sherman, *Hijacking the Internet is Far Too Easy* (Nov. 16, 2018), <https://slate.com/technology/2018/11/bgp-hijacking-russia-china-protocols-redirect-internet-traffic.html>; Dan Goodin, *Google goes down after major BGP mishap routes traffic through China* (Nov. 13, 2018), <https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/>; Dan Goodin, *Strange snafu misroutes domestic US Internet traffic through China Telecom* (Nov. 6, 2018), <https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom/>.

they assert that placing an untrusted entity in the position of a provider of international telecommunications service would be unacceptably disruptive to each of these activities.⁸³

28. The Executive Branch agencies have supported the validity of their concerns by pointing to certain undisputed statements that China Mobile USA itself made in its written responses to these agencies' inquiries in connection with this proceeding. According to the agencies, although China Mobile USA may **[BEGIN CONFID. INFO.]** **[END CONFID. INFO.]**, it would have numerous interconnection agreements with U.S. carriers.⁸⁴ China Mobile USA told the agencies **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.]⁸⁵ Furthermore, the Executive Branch agencies note that China Mobile USA **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.]⁸⁶ If China Mobile USA receives an international section 214 authorization, the China Mobile group **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.]⁸⁷ Given these planned interconnection arrangements—as well as connections to China Mobile USA's anticipated customers, including fixed and mobile network operators, wholesale carriers, calling card companies, phone line companies, and enterprise customers—the Executive Branch agencies state that they consider the risks to be unacceptable.⁸⁸ According to the agencies, the Chinese government could use China Mobile USA to conduct or to increase economic espionage and intelligence collection against the United States. Even if China Mobile USA **[BEGIN CONFID. INFO.]** **[END CONFID. INFO.]**, the agencies contend that the Chinese government could still exploit China Mobile USA's presence in the U.S. domestic telecommunications network and the resulting increased access to U.S. companies and data.⁸⁹

29. The Executive Branch agencies conclude that the Chinese government could use China Mobile USA's common carrier status “to exploit the public-switched telephone network in the United States and increase intelligence collection against U.S. government agencies and other sensitive targets that depend on this network.”⁹⁰ According to the agencies, the Chinese government, through China Mobile USA as a common carrier, would have a greater ability to monitor, degrade, and disrupt U.S. government communications. They note that China Mobile USA's application states that China Mobile

⁸³ Executive Branch Recommendation at 10-14.

⁸⁴ *Id.* at 15.

⁸⁵ *Id.* (citing Exhs. 1-2, Nov. 3, 2011 response from China Mobile USA to Executive Branch agencies' October 5, 2011 questions).

⁸⁶ *Id.* at 4-5 (citing Exhs. 3 & 4, April 27, 2012 response from China Mobile USA to Executive Branch agencies' Feb. 28, 2012 questions).

⁸⁷ *Id.* at 5, (citing Exhs. 3 & 4, April 27, 2012 response from China Mobile USA to Executive Branch agencies' Feb. 28, 2012 questions).

⁸⁸ *Id.* at 15.

⁸⁹ *Id.* China Mobile USA told the Executive Branch agencies that **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.].

Id. (citing Exh. 10, June 12, 2015 Mitigation Proposal from China Mobile USA).

⁹⁰ *Id.* at 10.

USA intends to offer its service to other carriers.⁹¹ They further observe that, due to least cost routing, if China Mobile USA were granted an authorization, the communications of U.S. government agencies to any international destinations may pass through China Mobile USA's network during transit, even if the agencies are not actual China Mobile USA customers.⁹²

30. Based on the record evidence, we are persuaded that there are valid national security and law enforcement concerns that apply to China Mobile USA's application. In particular, we find persuasive in the current security environment the argument that there is a significant risk that the Chinese government would use China Mobile USA to conduct activities that would seriously jeopardize the national security interests and law enforcement activities of the United States. Although there is no public record information that the Chinese government has used China Mobile or China Mobile USA for these purposes to date, there is clear evidence in the public record that the Chinese government has used other state-owned Chinese companies to act against U.S. interests. Given the Chinese government's ability to similarly exert influence and control over China Mobile and China Mobile USA and the Executive Branch agencies' assessment that the Chinese government would use these entities for activities counter to U.S. interests if the opportunity arises, we find this information relevant to our public interest review of the application.

31. We also agree that China Mobile USA's receipt of an international section 214 authorization would provide China Mobile USA with access to critical infrastructure. Such access by China Mobile USA, and by extension the Chinese government, would lead to significant additional risk to U.S. national security and law enforcement interests through, for example, espionage and intelligence activities. China Mobile USA's primary response to this issue is that any national security and law enforcement concerns can be addressed through mitigation.⁹³ As we discuss in the next section, we are persuaded that mitigation is not a viable option to address the national security and law enforcement risks in this instance. China Mobile USA also argues that it is not subject to influence or control by the Chinese government⁹⁴ and that the reports and other evidence provided in the Executive Branch Recommendation do not specifically pertain to China Mobile USA.⁹⁵

32. We find, however, that China Mobile USA has not rebutted the assessment that it is susceptible to such exploitation, influence, and control and that this raises valid national security and law enforcement concerns that apply to China Mobile USA's application. China Mobile USA provides no evidence to rebut the extensive showings made by the Executive Branch concerning past examples of conduct by the Chinese government that have raised substantial national security and law enforcement concerns, or the applicability of Chinese laws that would require China Mobile USA to comply with any requests made by the Chinese government,⁹⁶ but rather argues that these examples have not so far

⁹¹ Executive Branch Recommendation at 10.

⁹² *Id.*

⁹³ China Mobile USA Opposition at 8, 13-15.

⁹⁴ *Id.* at 9.

⁹⁵ *Id.* at 10-13.

⁹⁶ China Mobile USA argues that, as a Delaware corporation, it is "subject to U.S. law" and the Chinese government's ownership and control of it would therefore not require it "to comply with foreign government requests relating to its operations within the United States." *Id.* at 9. Though it would certainly be subject to U.S. law, China Mobile USA would also be managed by its board of directors and operated in the interests of its ultimate controlling shareholder. See 8 Del.C. § 141(a); see also *Cede & Co. v. Technicolor, Inc.* 634 A.2d 345, 360 (Del. 1993) ("[a] fundamental principle of Delaware law [is] that the business and affairs of a corporation are managed by or under the direction of its board of directors. In exercising these powers, directors are charged with an unyielding fiduciary duty to protect the interests of the corporation and to act in the best interests of its shareholders" (citations

(continued....)

involved China Mobile USA (which as yet has no such authorization).⁹⁷ Particularly as applied to a subsidiary ultimately controlled by the Chinese government, in light of the substantial concerns raised by the Executive Branch, and because of the serious nature of the risks posed by the grant of this application to U.S. critical infrastructure, national security, and effective law enforcement investigations, we find China Mobile USA's arguments unpersuasive.

33. Therefore, we conclude that significant national security and law enforcement harms would arise from granting China Mobile USA an international section 214 authorization that is not subject to effective mitigation.⁹⁸ Because, as discussed in the next section, we are persuaded that these risks cannot be mitigated, grant of the application would result in substantial and serious national security and law enforcement risks.

D. The National Security and Law Enforcement Risks Cannot be Addressed by Mitigation

34. The Executive Branch agencies contend that, given China Mobile USA's vulnerability to Chinese government influence, the current national security environment, China Mobile USA's plans to interconnect with the U.S. telecommunications infrastructure, and the sensitivity of that infrastructure to U.S. national security and law enforcement interests, the risks cannot be mitigated through a voluntary agreement.⁹⁹ China Mobile USA argues that any national security and law enforcement concerns with its application can be addressed through such means and adds that other state-owned enterprises have been able to enter into mitigation agreements and receive an international section 214 authorization, citing the grant of the applications of Telin USA and OPT French Polynesia.¹⁰⁰ China Mobile USA states that, on June 12, 2015, it provided the Executive Branch agencies with a detailed mitigation proposal,¹⁰¹ and asserts that the agencies have not demonstrated why the proposed mitigation terms are inadequate.¹⁰²

35. The Executive Branch agencies counter that their Recommendation does explain why the identified national security and law enforcement risks cannot be mitigated in the circumstances specific to

(Continued from previous page) _____

omitted)). The applicant also does not explain how, even if it were correct, its view of Delaware law could be enforced as a practical matter extraterritorially against the Chinese government.

⁹⁷ China Mobile USA Opposition at 9-15.

⁹⁸ China Mobile USA would be able to request interconnection with the networks of other U.S. common carriers. China Mobile USA has stated that if granted an international section 214 authorization it plans to provide international facilities-based and resale services to all international destinations (except those points on the Commission's exclusion list). *See supra* at para. 4. China Mobile USA has stated that a more limited grant of resale-only authority would not be acceptable. *Id.* at para. 4, n.17. China Mobile USA has also stated that it intends to offer international interexchange services, international private line circuits, and MVNO services. *Id.* at para. 4. The provision of some of these services may also include a domestic U.S. component. As stated above, China Mobile USA does not need an international section 214 authorization to offer domestic MVNO services. It does need such authority to transport the communications it receives as an MVNO operator from the United States to foreign points. *Id.* at para. 4, n.20. China Mobile USA also plans to offer a number of services in the United States that it states do not require an international section 214 authorization, such as data center and cloud services. *Id.* at para. 4; *see also* Executive Branch Recommendation at 5.

⁹⁹ Executive Branch Recommendation at 14-17; Executive Branch Reply at 15-19.

¹⁰⁰ China Mobile USA Opposition at 2, 15; *see also* China Mobile USA Oct. 6, 2014 *Ex Parte*, at 1 (asserting that "[t]he lack of international Section 214 authority places China Mobile USA at a competitive disadvantage vis-à-vis its U.S. and foreign competitors (including other Chinese carriers already authorized by the Commission to operate in the U.S. market in at least one case subject to assurances made to [the Executive Branch agencies]). . . .").

¹⁰¹ China Mobile USA Opposition at 4, 13, 15.

¹⁰² *Id.* at 13-15; China Mobile USA Nov. 21, 2016 *Ex Parte* Letter.

China Mobile USA's application, and the reasons underlying the conclusion apply to each of the proposed mitigation measures.¹⁰³ The agencies state that their evaluation of China Mobile USA's application included both a careful review of the mitigation approaches suggested by China Mobile USA as well as consideration of other potential mitigation approaches independently identified by the Executive Branch agencies.¹⁰⁴ The review focused on technical implications of the China Mobile USA application and whether a combination of various mitigation proposals would adequately address the law enforcement and national security risks.¹⁰⁵ The Executive Branch agencies respond to China Mobile USA's assertion that the Executive Branch has entered into mitigation agreements with other state-owned enterprises by noting that each applicant is evaluated based on the facts and circumstances relevant to the specific application. So, for example, when China Mobile USA informed the Executive Branch agencies that **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.], China Mobile USA's response was considered against the backdrop of its status as the subsidiary of a prominent Chinese state-owned enterprise, the size and technical and financial resources of China Mobile USA and its state-owned enterprise parent, the depth of its potential access to the U.S. telecommunications network as a common carrier, and the Chinese government's policy of utilizing state-owned enterprises and other enterprises to further its intelligence activities and economic espionage efforts.¹⁰⁶ Through this process, the Executive Branch agencies determined that the national security and law enforcement risks presented by granting China Mobile USA an international section 214 authorization cannot be resolved through a mitigation agreement in the current national security environment.¹⁰⁷

¹⁰³ Executive Branch Reply at 14-19 (noting "information as well as the mitigation proposals offered by China Mobile [USA], were carefully considered, analyzed, and discussed within the Executive Branch over the course of dozens of meetings."); *see also* China Mobile USA Opposition at 4 (noting extensive engagement with the Executive Branch agencies). The China Mobile USA proposal, which was extensively evaluated by the Executive Branch agencies, included: **[BEGIN CONFID. INFO.]**

[END CONFID. INFO.]. Executive Branch Recommendation at 16 (citing Exh. 10, June 12, 2015 Mitigation Proposal from China Mobile USA).

¹⁰⁴ Executive Branch Recommendation at 14-15.

¹⁰⁵ *Id.* at 14-17.

¹⁰⁶ Executive Branch Reply at 16 and n.55 (citing Exh. 3, Dec. 2, 2016 email from Kent Bressie to Executive Branch agencies) and n.56 (citing to the *House Report* on Huawei and ZTE at 2).

¹⁰⁷ Executive Branch Recommendation at 14-17.

36. Additionally, the Executive Branch agencies assert that mitigation agreements are only as strong as the U.S. government's ability to enforce their terms.¹⁰⁸ They state that the Executive Branch relies on a baseline level of trust when working with telecommunications carriers, due to the sensitivity of national security and law enforcement investigations.¹⁰⁹ They further state that despite regular compliance monitoring they can never have full visibility into all of the activities of a company, and necessarily rely on the other party to adhere rigorously and scrupulously to mitigation agreement provisions, and to self-report any problems of non-compliance.¹¹⁰ In this regard, they conclude that because China Mobile USA is subject to exploitation, influence, and control by the Chinese government, China Mobile USA could, at the behest of the Chinese government, violate the mitigation agreement as it may be required to do under Chinese law, and not self-report as required by the agreement (indeed, as also may be required under Chinese law¹¹¹).¹¹² Such breaches, they note, even if promptly discovered and resolved, very likely cannot be remediated.¹¹³ For example, disclosure to the Chinese government of national security or law enforcement requests or the unauthorized access to customer or company data could create irreparable damage to U.S. national security.¹¹⁴ They also contend that they would not be able to work effectively with China Mobile USA to identify and disrupt unlawful activities such as computer intrusions, or to assist in the investigation of past and current unlawful conduct, as the U.S. government does with trusted voice communication providers.¹¹⁵

37. As noted, in the current environment the Executive Branch agencies have greater knowledge of the risks of granting international section 214 authorizations to Chinese state-owned enterprises, including increased awareness of China's role in economic and other espionage against the United States.¹¹⁶ As a result, they have concluded that prior mitigation measures applied to certain Chinese state-owned companies would be insufficient here to address the risks posed by grant of an international section 214 authorization to China Mobile USA.¹¹⁷ The agencies add that mitigation "terms

¹⁰⁸ Executive Branch Reply at 16-17.

¹⁰⁹ *Id.* at 18; Executive Branch Recommendation at 13.

¹¹⁰ Executive Branch Recommendation at 16; Executive Branch Reply at 17-19.

¹¹¹ *See supra* para. 17 & n.55 (noting that Article 7 of the 2017 National Intelligence Law provides that "[a]n organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows" (emphasis added)).

¹¹² Executive Branch Recommendation at 16.

¹¹³ *Id.* at 16-17.

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 13. The Executive Branch agencies assert that there is a strong likelihood that China Mobile USA, as an international telecommunications provider, would have access to a significant amount of information, such as the contents of wire and electronic communications, that would be relevant to law enforcement and national security investigations. Executive Branch Reply at 12. Given this backdrop, the Executive Branch agencies are concerned that China Mobile USA's Chinese state-owned enterprise parent "may have particular sensitivities that will inform China Mobile USA's compliance with lawful process that seeks information transmitted using networks connected to China." *Id.* The Executive Branch agencies also express concern that China Mobile USA cannot be trusted to identify, disrupt, or provide assistance for investigations into unlawful activity that may involve or relate to the Chinese government given its status as a U.S. subsidiary with an indirect Chinese state-owned enterprise parent. *Id.* at 12-13.

¹¹⁶ Executive Branch Recommendation at 14.

¹¹⁷ *Id.*

and agreements that may have adequately protected national security five years ago may not address newly discovered risk in today's rapidly evolving threat environment."¹¹⁸

38. Any Commission grant of the pending international section 214 application would need to find that China Mobile USA's provision of global facilities-based and resale common carrier services on U.S.-international routes is in the public interest, despite the national security and law enforcement risks identified by the broad coalition of Executive Branch agencies as being unmitigable. Given the evidence in the record, we are persuaded that the underlying foundation of trust that is needed for a mitigation agreement to adequately address national security and law enforcement concerns is not present in the instant case. In this regard, we acknowledge the Executive Branch's established role in monitoring and enforcing compliance with mitigation agreements and, therefore, we conclude that it is appropriate to defer to what we believe to be a reasonable assertion of the Executive Branch agencies that mitigation is not an adequate option here. We therefore conclude, for the purpose of our public interest analysis in this proceeding, that absent the ability to mitigate, any Commission grant of China Mobile USA's application to provide global facilities-based and resale services on U.S.-international routes would not serve the public interest, in light of the Chinese government's likely intention and ability to use the international section 214 authorization to cause substantial harm to U.S. critical infrastructure, national security, and law enforcement activities. Therefore, we deny the application.

IV. ORDERING CLAUSES

39. Accordingly, IT IS ORDERED, pursuant to sections 4(i), 4(j), and 214 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 154(i), (j), 214 and sections 63.12, 63.18, and 63.21, of the Commission's rules, 47 CFR §§ 63.12, 63.18, and 63.21, that the international section 214 authorization application under File No. ITC-214-20110901-00289 IS HEREBY DENIED.

40. Petitions for reconsideration under section 1.106 of the Commission's rules, 47 CFR § 1.106, may be filed within 30 days of the date of the release of this Memorandum Opinion and Order.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

¹¹⁸ Executive Branch Reply at 16.

APPENDIX A

Classified Supplement

**STATEMENT OF
CHAIRMAN AJIT PAI**

Re: *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, ITC-214-20110901-00289*

Last week, I was honored to be part of the United States delegation to an international conference on 5G network security hosted by the Czech Republic. There was a broad consensus at this gathering that network security is not only a priority but a necessity. And through close collaboration among over 30 nations, the conference produced a set of 5G security principles that reflect the common understanding that the “security of 5G networks is crucial for national security, economic security and other national interests and global stability.”¹ This was a major accomplishment and concrete evidence of the progress the Administration has made on the international stage on this issue.

The work that we are doing here at home also is vital to ensuring that wireless networks are safe and secure. Along those lines, I joined several other Administration officials yesterday in a detailed briefing of members of the Senate Select Committee on Intelligence. While I can’t discuss what transpired at the meeting, I can say that at the intersection of national security and communications lies a strong bipartisan consensus in favor of proactive measures to protect our networks at the front end, not as an afterthought.

Another facet of the FCC’s domestic work involves ensuring that foreign entities seeking to provide telecommunications services in the United States do not pose a risk to our national security. And that brings us to the matter at hand.

In 2011, China Mobile USA applied to the FCC seeking to provide international telecommunications services in the United States. As we normally do, we asked the Executive Branch for its views on this application. After a lengthy review process, the Executive Branch last year recommended that we deny the application for national security and law enforcement reasons. And after carefully reviewing the record, I agree that rejecting China Mobile’s application is the right call.

Simply put, granting China Mobile’s application would not be in the public interest. China Mobile ultimately is owned and controlled by the Chinese government. That makes it vulnerable to exploitation, influence, and control by that government. And in the current security environment, which features Chinese government involvement in computer intrusions and economic espionage, there is a significant risk that the Chinese government would use China Mobile to conduct activities that would seriously jeopardize the national security, law enforcement, and economic interests of the United States. Among other things, if this application were granted, 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. That is a flatly unacceptable risk.²

I will put it plainly: When it comes to our national security, we cannot afford to make risky choices and just hope for the best. We must have a clear-eyed view of the threats that we face and be

¹ The Prague Proposals issued following the Prague 5G Security Conference are available at <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>.

² Aside from the risks that flow from direct ownership in this case, Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts throughout the world. As a result, China Mobile would likely comply with espionage and intelligence requests made by the Chinese government.

prepared to do what is necessary to counter those threats. That's exactly what the Commission is doing today in denying China Mobile's application.

I would like to thank the Executive Branch agencies that provided us with their feedback as well as the following FCC staff who worked on this item: Denise Coca, Kate Collins, Kimberly Cook, Veronica Garcia-Ulloa, Francis Gutierrez, David Krech, Artie Lechtman, Ron Marcelo, Adrienne McNeil, Thomas Sullivan, and Troy Tanner from the International Bureau; David Horowitz, Doug Klein, Bill Richardson from the Office of General Counsel; Heidi Kroll, Virginia Metallo, and Emily Talaga from the Office of Economics and Analytics; Jeff Goldthorp and Deb Jordan from the Public Safety and Homeland Security Bureau; and Mary Harmon and Raenell Plummer from the Office of the Managing Director.

**STATEMENT OF
COMMISSIONER MICHAEL O'RIELLY**

Re: *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, ITC-214-20110901-00289*

Those who follow FCC proceedings may notice that I often start or finish meeting item statements by saying that I am pleased to support or approve this or that order, NPRM, or public notice under consideration. While I will vote in favor of today's item, I do not derive any joy from doing so due to the weighty nature of this issue. As a fierce supporter of promoting competition, permitting foreign ownership, and facilitating open markets, I nonetheless find the situation confronting us to be extremely serious, and the action we take today to block China Mobile from accessing the U.S. telecommunications market to be a necessary step, drastic though it may be. Being a fervent free trader, I strongly believe that participating in open markets comes with corresponding obligations to comport within established norms. That principle applies to all countries and providers, irrespective of their domestic form of government.

As I read it, our action today is consistent with a speech I gave two weeks ago discussing the many fundamental concerns I have about Chinese government attempts to monopolize 5G development and deployment. One basic reality should go undisputed: there is nearly zero daylight between the communist government of China and its "companies." They use unfair advantages in an effort to take a dominant position in 5G and expand the reach of their networks and equipment. By providing improper government subsidies, throwing cheap labor at service projects, and stealing intellectual property, among other unsavory and illegal tactics, China effectively offers competitive products and services below cost, allowing wireless providers and manufacturers to gain market share not only in China but internationally. Further, the pervasive presence of Chinese equipment and providers in a nation's communications marketplace places these countries' national security at risk.

Today's order sets forth a convincing case for why permitting China Mobile to provide telecommunications services between the U.S and foreign locations is not in the public interest. The item details why China Mobile is "vulnerable to exploitation, influence, and control" by the Chinese government, which could seriously jeopardize U.S. national security and law enforcement interests.¹ Providing China Mobile with greater access to U.S. telephone lines, fiber-optic cable, and wireless networks will give China – with its track record of computer intrusions, economic espionage and other ongoing intelligence activities – access to information carried over these networks and the ability to disrupt communications. In fact, Chinese law requires organizations "to support, assist in, and cooperate in China's national intelligence work,"² "wherever they operate."³

As part of our general process, the Commission sought input from the national security, law enforcement, and foreign and trade policy experts that comprise what is known as "Team Telecom." Team Telecom found substantial national security and law enforcement risks that could not be mitigated and requested that the Commission deny the application. While the Commission performs its own review, I acknowledge the expertise of these Executive Branch agencies when it comes to national

¹ *Supra* para. 8; *see also supra* para. 14.

² National Intelligence Law of the P.R.C. (2017), Article 7; *see also supra* para. 17.

³ Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019, at 101 (May 2, 2019), https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

security issues, recognize the value of their review, and agree with their conclusion. I appreciate the collective insight they provided into this important matter.

At the same time, there is little dispute that Team Telecom must improve the transparency and timeliness of their decisions. By way of background, this particular application was filed on September 1, 2011, and NTIA didn't file the recommendation to deny it, on behalf of Team Telecom, until July 2018. I understand that these issues are complex, but all applicants deserve timely responses, and this decision, while inevitable, was far from timely. Luckily, those on the inside of Team Telecom are finally recognizing some of the deficiencies in this process. Recently, a leading figure within the Department of Justice's National Security Division, which is a key member of Team Telecom, stated publicly that "we must reform the ad hoc process by which the Executive Branch advises on FCC licenses" in order to "explore ways to make this process more efficient and expedient, so that the Executive Branch never again takes nearly seven years to make a recommendation."⁴ Of note, I have been calling for Team Telecom reform since 2015 and worked closely with former Chairman Wheeler on a proceeding to adopt deadlines and enhance transparency, only to have him inexplicably pull the plug a day or two after the 2016 election. I strongly believe in codifying the structure of Team Telecom and streamlining its procedures, and this can be done without jeopardizing our national security or undermining our ability to protect U.S. interests. I look forward to further action on this matter, whether internally at the FCC or by the Administration itself.

Finally, certain perpetual critics have taken today's item as an opportunity to suggest that, while it is nice for the Commission to take this step to ensure our national security, it has not done enough to impose strict network security regulations on the provision of 5G wireless services. Some may even go further and demand that today's order affirmatively mandate new burdens to address general issues regarding 5G security. That is an intentional attempt to conflate issues and mangle the situation. Today's order considers the national security implications raised by China Mobile's international 214 *application*. This is not a rulemaking of general applicability, but a fact-specific adjudication raised by one individual entity's request. In other words, a particular application may have significant implications for national security, but it does not form the basis for taking far-reaching action. A consideration of national security implications is certainly within the Commission's authority when considering licensees with significant foreign investment, and it is consistent with the FCC's section 214 review process, but the question of how to secure the nation's communications networks is a broader matter, distinct from the issues we consider today.

Separately, I would note that American wireless providers have been working hard to ensure robust security as part of their 5G offerings, including through the standards process. These entities appreciate that security is critical to consumers' and end users' comfort and willingness to use their underlying networks. Thanks to competition, providers have the incentive to provide the most secure network possible.

Moreover, Congress has time and again decided that network security issues are to be led and handled by other federal agencies, particularly the Department of Homeland Security. Shoehorning network security into the Commission's jurisdiction amounts to a misreading of the statute and ignores congressional intent. If, in the future, Congress decides that the Commission should have this authority, I will be more than happy to take up this issue.

⁴ Deputy Assistant Attorney General Adam S. Hickey, National Security Division, Department of Justice, Remarks at the Fifth National Conference on CFIUS and Team Telecom (Apr. 24, 2019), <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-adam-s-hickey-national-security-division-delivers-0>.

In the end, the action we take today is justified. If circumstances change substantially, I am sure the Commission will have the opportunity to revisit the matter, as appropriate.

**STATEMENT OF
COMMISSIONER BRENDAN CARR**

Re: *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, ITC-214-20110901-00289*

The free market is building the next generation of communications networks in America. Broadband providers have invested \$1.6 trillion in connecting households to fast Internet. And wireless carriers are spending more than \$30 billion per year to upgrade to 5G.

Investors are willing to put that astonishing amount of capital at risk to serve American families because of the open system we have. Our economy is vibrant because people around the globe have confidence that we will uphold the rule of law. We are the top destination for foreign direct investment, attracting \$4 trillion—money used to employ our scientists in R&D, our tradesmen in construction, and our farmers in their efforts to feed the world. If you play by the rules here, we welcome your business. That commitment has been at the foundation of our success as a country.

And so in telecom, we don't have nationalized networks. The government's role is to encourage all comers to invest, build, and serve Americans—so long as they play by the rules. The government acts as the referee, not the star player. And in this case, it's imperative that we blow the whistle.

When a company seeks authorization to integrate itself into our communications networks, our security review must consider at least three questions. First, how much control can a foreign actor exert over the company? Second, what evidence do we have about the foreign actor's desire to exercise that control? And, third, if the foreign actor were to act on its malintent, what's the scope of the threat that the specific authorization poses?

Here, the answer to the first question is clear. The People's Republic of China owns China Mobile. The Chinese government controls its management and can direct its actions. Compounding its control by ownership, the Chinese government can compel access to telecom facilities within China on demand. China's 2017 National Intelligence Law mandates that "[a]ll organizations and citizens . . . support, assist, and cooperate with national intelligence efforts in accordance with law." We understand that this vague dictate places Chinese telecoms and their customers under routine and secret surveillance by the People's Republic of China.

Second, we have substantial evidence that the Chinese government intends to surveil persons within our borders, for government security and spying advantage, as well as for intellectual property and a business edge. Just this week, the New York Times reported that hackers working for the Chinese government stole some of our government's most important cybersecurity tools and repurposed them to attack Western allies and businesses. The Chinese reportedly targeted an ally's telecom network, and when the tools were later transferred to North Korea and Russia, those governments crippled British hospitals and shipping companies. They even shut down a Ukrainian airport, its postal service, gas stations, and ATMs. There is little doubt that the Chinese government would value additional direct access to our telecom networks for reasons contrary to our security interests.

Third, we must assess the scope of the U.S. authorization at issue. In this case, the Chinese government, through China Mobile, proposes to carry traffic from our shores to international destinations.

The purported business plan is to provide low-cost calls between the U.S. and China. At first blush, this looks like a narrow authorization. Interconnection is not integration, and, in any case, we may assume some security risk whenever traffic goes abroad. This reasoning might be dispositive if interconnection were that simple. But due to least-cost routing, a customer may not be able to choose which company carries the traffic. And once on a particular carrier, the traffic can follow a path of the carrier's choosing. This is what security researchers discovered in November, when Internet traffic originating in Los Angeles and destined for Washington, D.C. was sent on a detour through Hangzhou, China. The Chinese government owns the company that directed the traffic along the puzzling LA-Hangzhou-D.C. route.

So the evidence in this case is clear. After a multi-year inquiry spanning two administrations, the Executive Branch agencies recommended that the FCC deny China Mobile's application due to national security and law enforcement concerns—the first such recommendation, ever. The record here supports that outcome.

In fact, the evidence suggests that we should go even further. The Chinese government owns a number of other carriers that already are operating in the U.S., including China Unicom and China Telecom. Those companies hold the same Section 214 authorizations that China Mobile sought. The evidence I've seen in this case calls those existing authorizations into question. For instance, the decision today cites reports that China Telecom has been hijacking U.S. traffic and redirecting it through China.

So it's time for the U.S. to take additional action. Our national security agencies should examine whether the FCC should revoke those existing Section 214 authorizations, and the FCC should open a proceeding on those matters. Security threats have evolved over the many years since those companies were granted interconnection rights to U.S. networks in the early 2000s. Much if not all of the reasoning behind today's decision appears to apply with equal or greater force to those legacy authorizations. Let's ensure that our decisions from decades past don't inadvertently endanger American interests.

I thank the International Bureau for its work on this item. And I thank Team Telecom for its input. The item has my support.

**STATEMENT OF
COMMISSIONER JESSICA ROSENWORCEL**

Re: *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, ITC-214-20110901-00289*

Here's a hard truth: Today no communications system is ever fully secure.

To understand why requires a bit of history. For most of the twentieth century, communications in the United States was synonymous with a single company. That company's monopoly status meant that it controlled all aspects of security for the public switched telephone network. Moreover, communications traffic traveled by and large over buried cable, which provided a degree of physical protection from intrusion.

Then in 1984, courtesy of a court decision, we introduced competition to the communications marketplace. Lower prices and greater innovation followed. But this move also multiplied the number of actors and exponentially increased our security challenges.

The rise of consumer wireless communications came a bit later. Because wireless signals spread as they travel, they are easier to intercept. On top of this, the reliance on cell phone towers made it easy for bad actors to target network providers. Even today, many of these structures have limited physical security.

But the most profound change may be the rise of the Internet. As our lives migrated online, our communications combined control and content into a single channel, vastly simplifying the ability to attack a network and its users. Today the Internet underlies nearly every facet of our lives and is the foundation for much of the critical infrastructure that keeps our country running. But all of this activity is vulnerable to malicious software, denial-of-service attacks, form-jacking, phishing, and a growing range of application vulnerabilities. Billions of people were affected by cyber attacks last year and those numbers are only going to grow.

I started with a hard truth about security and our communications networks—that given the powerful complexity of modern communications, no system is ever fully secure. But that does not excuse us from working to improve the strength and resiliency of our networks. History demonstrates that as our communications capabilities evolve, so do their security risks. It is imperative that we make security a priority and build it into everything we do. So here's another hard truth: The Federal Communications Commission is doing too little to address the vast challenges of network security and safety.

I believe the first duty of the public servant is the public safety—and on that score this agency has work to do.

Please don't get confused by the performative security associated with this decision. This application has been in these halls for more than eight years. It has been on permanent pause. So while I support this vote, it does nothing to change the status quo. Nor does it address any of the fundamental challenges to the security of digital age communications.

To move beyond performative security to real security, this agency needs to change course. This is the right moment to do it. We are at an inflection point as the world races to deploy next-generation wireless networks. With 5G service, we will have wireless capability built into the world around us. This

will provide a whole new range of opportunities for civic and commercial life. But as they multiply, this will vastly expand our surface exposure to attack.

It is no longer enough for the United States to be first to 5G. If we want to ensure our continued technology leadership, the networks we deploy must also be secure. In a speech at the start of this year at the Center for Strategic and International Studies, I offered three ideas about just where the FCC can begin.

First, I suggested that the agency needs to re-charter and reinvigorate the Communications, Security, Reliability, and Interoperability Council and give it a new focus on 5G security. This needs to include more study on security technologies to reduce the risk from the Internet of Things, more study on network function virtualization to reduce denial-of-service attacks, and a new study on supply chain risk management that recommends specific mitigation techniques. Today, a bipartisan group of members from the House of Representatives sent this agency a letter calling for just this approach with the next iteration of this council. I support it and I hope my colleagues will follow my lead.

Second, late last year, the Department of Homeland Security announced the creation of the nation's first Information and Communications Technology Supply Chain Risk Management Task Force. This group is charged with developing national recommendations to identify and manage risk in the global supply chain for communications.

The task force includes officials from the Department of Homeland Security, Department of Defense, Department of Treasury, General Services Administration, Department of Justice, Department of Commerce, Office of the Director of National Intelligence, and the Social Security Administration. In addition, there is expertise from industry, with representatives from communications carriers, equipment manufacturers, and cybersecurity companies.

It's an impressive list, to be sure. But there's one agency that is missing. The FCC needs a prominent seat at this table. Leaving the agency with primary oversight over communications out is neither prudent nor wise. Good things come to those who ask, so it is time for this agency to insist that one of the individuals on this dais to join the leadership of this effort. Moreover, the work of this forum should inform our ongoing proceeding concerning equipment supported by universal service funds.

Third, the FCC needs to make cyber hygiene a priority. To keep our communications systems functioning we are going to need routine practices that increase security and reduce exposure to attack. The agency must build these policies into its day-to-day work. As the number of devices using radiofrequency expands with the Internet of Things, the agency should use its equipment authorization process to encourage device manufacturers to build security into new products. On top of this, the agency could ask that as a condition of holding a public license, licensees certify that they have implemented the best practices for 5G security. This could include a commitment to using the National Institute of Standards of Technology Cybersecurity Framework. While we're at it we need to do more to educate citizens about cyber hygiene. We must increase our outreach with consumers and consumer groups on the basics of cyber hygiene—from downloading software upgrades for devices to assessing connection security when using unlicensed airwaves.

Finally, the honest truth is that we have failed the public when it comes to the privacy and security of wireless devices. Reporting last year and earlier this year indicated that for a few hundred dollars a range of shady middlemen can tell you where any wireless phone is being used within a few hundred meters. Going forward, the potential for abuse is frightening. Remember, new wireless devices will be in our homes—from smart thermostats to virtual assistants to televisions with cameras and microphones. They will be outdoors—from smart electricity grids to adaptive traffic signals. They will

be in our cars, sensing engine operation and location. And they will inform the way we work, shop, seek healthcare, and engage with the world around us. Yet this agency has been silent when it comes to what happened that resulted in location aggregators getting this information from wireless carriers and making it available for purchase. This is an issue of personal and national security. This agency owes it to the American public to explain just what is going on with the privacy of our wireless devices.

Hard truths can make us uncomfortable. But our history shows that if we acknowledge them, they can be a call to action. I think it is time for this agency to act like network security and consumer privacy is a priority. I hope my colleagues are ready to change course and make this happen.

**STATEMENT OF
COMMISSIONER GEOFFREY STARKS**

Re: *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, ITC-214-200110901-00289*

It's a truism to state that we live in an interconnected world. But the security environment of today is very different from what we had before the '96 Act, in which a limited number of well-established carriers interconnected with each other. Network security in those days was primarily based on simple trust, not unlike neighbors in a small town leaving their back doors open. All the players knew each other so there wasn't much risk of anyone acting maliciously.

As communications technology has evolved and new parties have entered the network, the telecom "neighborhood" has become larger and more dangerous. While the great majority of newer network participants uphold the high security standards followed by the original small group of "trusted" entities, that low security trust-based environment has become more nostalgic than practical.¹ Numerous opportunistic bad actors now have ready access to network credentials that were once limited to trusted entities. As the Executive Branch agencies state in their Recommendation regarding the application at issue here:

This network was created with minimal security features because it was assumed that only trusted parties would have access. However, this lack of security features has led to law enforcement and national security vulnerabilities, such as giving an entity with access the ability to target, alter, block, and re-route traffic.²

Given our growing reliance on communications networks to support our critical infrastructure, transportation, health care and financial sector, the need for strong Commission action to address these security vulnerabilities has never been greater. Our authority is clear, beginning with Congress's explanation in Section 1 of the Communications Act of 1934 that it created the FCC both "for the purpose of the national defense" and "for the purpose of promoting safety of life and property."³ While some have suggested that Section 1 is merely a "policy statement," the Commission has long relied upon it as informing the public interest analyses performed in numerous circumstances under both Democratic and Republican leadership, including in Section 214 proceedings like the one before us today, in our consideration of proposed transfers of broadcast and wireless licenses,⁴ and in the *Supply Chain NPRM* adopted by this Commission last year.⁵

¹ See Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T to Senator Ron Wyden dated Oct. 13, 2017 at 1 ("At its inception, in the 1970s roughly 10 trusted carriers worldwide had access to the SS7 network. With the explosion of competition, international calling and roaming, hundreds of carriers now have access to SS7, many of them in unstable or unfriendly nations where credentials can be compromised - and, as you note, even sold on the open market for a fee. AT&T has therefore hardened and tuned our defenses to account for these developments given that the trust model is no longer fully reliable."), *available at* <https://www.wyden.senate.gov/imo/media/doc/ATT%20SS7%20Response.pdf>.

² Executive Branch Recommendation at 10.

³ 47 U.S.C. § 151.

⁴ See *Market Entry and Regulation of Foreign-Affiliated Entities*, Report and Order, 11 FCC Rcd 3873 para. 222 (1995); 47 U.S.C. § 310(d)(4) (prohibiting the grant of an FCC license to an entity exceeding the foreign ownership benchmark "if the Commission finds that the public interest will be served by the refusal or revocation of such license"); *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market; Market Entry and Regulation of Foreign-Affiliated Entities*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891,

(continued....)

Nor does our authority stop there. The Act expressly gives the Commission the authority to “perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this Act, as may be necessary in the execution of its functions,” and to “make such rules and regulations . . . as may be necessary in the execution of its functions.”⁶ Protecting our networks from persistent and potentially catastrophic security threats is the essence of “necessary.” Congress also has specifically required the Commission to ensure that both carriers and cable operators protect the confidentiality of their customers’ data.⁷ Such protections, by necessity, demand secure networks.⁸

I therefore will approach any matters raising national security concerns with this authority in mind. In any such proceeding, I will review the record before me and independently assess whether the proposed outcome protects the national defense and the safety of life and property. Having come from the Department of Justice, I greatly respect the expertise of the Executive Branch agencies and will carefully consider their views and any intelligence they acquire. Nevertheless, this agency must exercise its own judgment in light of our congressional responsibilities.

With that in mind, we come to China Mobile’s application for international Section 214 authority. As the item states, with a Section 214 authorization, China Mobile would be able to connect to the US

(Continued from previous page) —————

23918-21, paras. 59-66 (1997) (finding that national security is a factor under the Commission’s public interest analysis for both Section 214 authorizations and Section 310(b)(4) determinations); *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to Assign or Transfer Control of Licenses and Authorizations*, Memorandum Opinion and Order, 31 FCC Rcd 6327, 6521, para. 429 (2015) (considering applicant’s cybersecurity practices as part of the Commission’s public interest standard for evaluating merger applications under Section 214(a) and 310(d) of the Act).

⁵ *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket 18-89, Notice of Proposed Rulemaking, FCC 18-42 para. 36 & n.63 (rel. Apr. 17, 2018) (*Supply Chain NPRM*) (relying in part on 47 U.S.C. § 201(b)’s “public interest” authority, and citing Section 1; “Indeed, Congress similarly determined that promoting the national defense is an important public interest in section 1 of the Act, which describes the development of a ‘Nation-wide . . . wire and radio communication service, for the purpose of the national defense’ as one of the reasons for establishing the Commission.”).

⁶ See 47 U.S.C. §§ 154(i), 303(r). Additionally, the Supreme Court has repeatedly affirmed that the Commission can adopt regulations that are reasonably ancillary to the effective performance of its responsibilities. See *National Cable & Telecommunications Assn. v. Brand X Internet Services*, 545 U.S. 967 (2005); *United States v. Southwestern Cable Co.* 392 U.S. 157, 181 (1968).

⁷ 47 U.S.C. §§ 222, 551(c)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007) (carriers must use “every reasonable precaution” to protect customer data); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12525 para. 24 n.61 (1996) (“[I]n the Cable Communications Policy Act of 1984, Congress . . . sought to restrict unauthorized use of personally identifiable information [PII] by cable operators.”). See also 47 U.S.C. § 35; Exec. Ord. No. 10530 § 5(a) (May 10, 1954) (delegating authority to the Commission to issue submarine cable landing licenses upon a determination that, among other factors, such action “will promote the security of the United States”).

⁸ See *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers’ Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 at para. 36 (2007) (“[W]e make clear that carriers’ existing statutory obligations to protect their customers’ CPNI include a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.”).

telecom network and gain enhanced access to our telephone lines, fiber-optic cable, cellular networks and communications satellites. If it offers the least costly path to carry traffic on a particular route, China Mobile could even end up carrying the communications of US government agencies.

In light of the national security concerns convincingly raised here by the Executive Branch agencies and China Mobile's failure to allay those concerns, I fully support this item. But we have much more work to do if we are to fulfill our statutory duty to protect our telecommunications networks.

First, as the decision acknowledges, earlier Commissions granted international 214 authority to other carriers with similar ownership structures to that of China Mobile. The Executive Branch agencies, however, underscore how the national security environment has changed since those applications were granted, and that the risks associated with granting China Mobile's application are now heightened. It is a top priority for me to address any similar concerns Executive Branch agencies may have with other carriers. My colleagues and I should work together to do this important, and statutorily required, work.

Second, as noted earlier, a little more than one year ago, the Commission proposed to prohibit the use of USF funds for the purchase of equipment or services from any company that poses a national security threat to the integrity of US telecommunications networks or the communications supply chain.⁹ While the NPRM applies only prospectively and does not require the elimination of existing equipment, Congress subsequently passed the 2019 National Defense Authorization Act, which expressly prohibits agencies, including the FCC, from obligating or expending loan or grant funds to procure or obtain equipment, services or systems that use telecom equipment by specified Chinese companies under certain conditions.¹⁰ I firmly believe that the same security concerns raised here today are presented wherever this equipment is currently in our network. We are charged to act quickly to identify potential risks, take appropriate remedial action, and ensure that we address the needs of small rural carriers that may have this equipment in their systems. Our national security demands that we act decisively.

Finally, and more broadly, I believe the Commission needs to do more to protect the security of our telecommunications networks. As I noted earlier, Congress has charged our agency with protecting the national defense and the safety of life and property. While we may share this role with our federal partners, this agency still has the responsibility and expertise to ensure that carriers comprehensively protect the security of our telecommunications networks. As the Commission's Communications, Security, Reliability and Interoperability Council (CSRIC) has noted, both legacy and new networking systems are vulnerable to exploits like location tracking, interception, denial of service attacks and account fraud or modification.

While private sector action on these issues is laudable, the Commission needs to do more than cheer from the sidelines. We know that more steps to securing our networks are needed. According to DHS, all U.S. networks are vulnerable to surveillance by exploiting flaws in the SS7 authentication and authorization system.¹¹ Another study reports that one in three networks is at risk of fraud attacks like the scam where someone fools the network into forwarding them your bank's texts confirming your consent

⁹ *Supply Chain NPRM*.

¹⁰ See *Wireline Competition Bureau Seeks Comment on Section 889 of John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Public Notice, WC Docket 18-89 (rel. Oct. 26, 2018).

¹¹ Department of Homeland Security, "Study on Mobile Device Security" at 77 (April 2017) ("[DHS] believes that all U.S. carriers are vulnerable to these exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national essential functions.") available at <https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf> (last visited May 7, 2019).

to a big withdrawal.¹² In light of these circumstances, the Commission needs to answer the following questions, among others:

- How do we address the continued operation of legacy 2G and 3G networks with known cybersecurity flaws, given that these networks can be used as entry points for attacks on more current networks? Are there particular vulnerabilities to the rural and low-income consumers who use those legacy networks?
- What measures can we take to ensure that all carriers properly utilize the security measures available in state-of-the art networks?
- How do we ensure that communications networks that receive USF support or that carry federal government communications are protected against security threats?
- How do we identify and fix any security flaws with 5G networks before their widespread deployment?

As noted above, our communications networks already underpin our utilities, transportation, financial system and health care. With this comes great responsibility. As we move into a world of 5G and the Internet of Things, our network grows larger and more interconnected than ever, and real risks and the potential harm of telecom network vulnerabilities will grow exponentially.

The days when our telecom networks could be likened to a small town safely organized around neighborly trust are long gone. We're in a new neighborhood full of both threats and opportunities, and the Commission's policies need to reflect that reality. I will be a strong voice for such change.

Thank you to the International Bureau for your excellent work on this item.

¹² Positive Technologies, "Diameter Vulnerabilities Exposure Report 2018," (June 14, 2018), *available at* <https://www.ptsecurity.com/ww-en/analytics/diameter-2018/> (last visited May 6, 2019).