UNITED STATES DEPARTMENT OF COMMERCE
National Telecommunications and
Information Administration
Washington, D.C. 20230

November 16, 2020

Ms. Denise Coca
Chief, Telecommunications and Analysis Division
International Bureau
Federal Communications Commission
45 L Street, N.E.
Washington, DC 20554

Re: Pacific Networks Corp. and ComNet (USA) LLC
GN Docket No. 20-111
ITC-214-20090105-00006 and ITC-214-20090424-00199

Dear Ms. Coca:

The National Telecommunications and Information Administration (NTIA), on behalf of the Executive Branch, provides the following response to the Federal Communications Commission ("FCC" or "Commission") to address the arguments made by Pacific Networks Corp. ("Pacific Networks") and ComNet (USA) LLC ("ComNet" and together with Pacific Networks, the "Companies") in the Companies' response to the FCC's April 24, 2020, *Order to Show Cause*.[1] This letter responds to the Commission's request for a response by the Attorney General in his role as Chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector ("Committee") under Executive Order 13913.[2] Given the nature of the Commission's request for views on discreet factual questions, and the limited time allotted for response, this response is not offered as a recommendation by the Committee, pursuant to Section 6 of E.O. 13913, that the FCC take any particular action with respect to the Companies. Instead, interested Executive Branch entities[3] offer the following views pursuant to their discretion to communicate information to the FCC. *See, e.g.*, E.O. 13913, §§ 10(h)(ii), 12(a)(i).

---

[1] *Pacific Networks Corp. and ComNet (USA) LLC,* Order to Show Cause, GN Docket No. 20-111, ITC-214-20090105, ITC-214-20099424-0199 (rel. Apr. 24, 2020)

[2] Exec. Order No. 13913, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643 (Apr. 8, 2020).

[3] The interested Executive Branch agencies for purposes of this response include the Department of Justice, Department of Homeland Security, Department of Defense, Department of Commerce, Department of the Treasury, Department of State, Office of Management and Budget, Office of the U.S. Trade Representative, General Services Administration, and Council of Economic Advisers.

Inherent national security risks attach to telecommunications companies owned or controlled by the Chinese government, and they have increased significantly in recent years. We provide our views regarding whether the Companies are subject to the exploitation, influence, and control of the Chinese government, and the national security and law enforcement risks associated with such exploitation, influence, and control. These risks will come as no surprise to the FCC, as the same risks were applicable and were identified in detail in the recommendation submitted to the FCC concerning China Telecom Americas Corporation's ("China Telecom") international Section 214 authorizations.[4] Further, the United States Senate's Permanent Subcommittee on Investigations stated in a recent report ("PSI Report") that "[t]he national security concerns Team Telecom and the [Commission] outlined in relation to China Mobile USA are applicable to the Chinese state-owned carriers currently operating in the United States."[5] The Companies are ultimately owned and controlled by CITIC Group Corporation ("CITIC"), a Chinese state-owned limited liability corporation.[6] As recently articulated by the Commission, there is significant risk the Chinese government would use certain Section 214 authorizations granted to Chinese state-owned carriers to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States.[7] The Companies' international Section 214 authorizations are conditioned on ongoing compliance with a 2009 Letter of Assurance ("Letter of Assurance") with the Department of Justice ("DOJ") and the Department of Homeland Security ("DHS", and, together with DOJ, the "Monitoring Agencies"). However, framed by the Commission's articulation of current national security concerns, those mitigation conditions would not address the current law enforcement and national security risks identified both by Congress and the Commission.

The national security environment has changed significantly since 2009, when the Commission last granted the Companies' Section 214 authorizations to provide international common carrier services. Then, more than a decade ago, the U.S. Intelligence Community's top concerns were the global economic crisis and violent extremism.[8] Although the Office of the Director of National Intelligence ("ODNI"), in its annual threat assessment, briefly identified the

---

[4] *Exec. Branch Recommendation to the Fed. Commc'ns Comm'n to Revoke and Terminate China Telecom's Int'l Section 214 Common Carrier Authorizations,* File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (filed Apr. 9, 2020) (hereinafter "Exec. Branch Recommendation to Revoke China Telecom").

[5] Staff of S. Permanent Subcomm. on Investigations, 116th Cong., *Threats to U.S. Networks: Oversight of Chinese Gov't-Owned Carriers* 5 (Comm. Print. 2020) (hereinafter "PSI Report").

[6] Order at 2-3. *See generally Pacific Networks Corp. and ComNet (USA) LLC,* Response to Order to Show Cause, GN Docket No. 20-111, ITC-214-20090105, ITC-214-20099424-0199 (June 1, 2020) ("Response to Order to Show Cause").

[7] *See generally China Mobile International (USA) Inc.; Application for Global Facilities-Based and Global Resale Int'l Telecomms. Auth. Pursuant to Sec. 214 of the Comms. Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd 3361 (2019) (hereinafter "China Mobile Order").

[8] *See Annual Threat Assessment of the Intelligence Comm. for the S. Select Comm. On Intelligence*, 111th Cong. 38-39 (2009) (statement of Dennis C. Blair, Director of National Intelligence), https://www.dni.gov/files/documents/Newsroom/Testimonies/20090212_testimony.pdf.

growing threat to U.S. information infrastructure posed by state and non-state adversaries, China's role in this growing threat was only mentioned in passing.[9]

In 2020, the top threats facing the United States are different – cyber issues now dominate the ODNI's threat assessment, with China being the first country identified by name for its persistent economic espionage and growing threat to core military and critical infrastructure systems.[10] The ODNI's threat assessment revealed the culmination of years of aggressive behavior by the Chinese government and the concomitant counterintelligence challenges confronting the United States. In July 2018, one year before the 2019 ODNI Worldwide Threat Assessment was published, the Director of the Federal Bureau of Investigation ("FBI") described the magnitude of the national security threat the Chinese government presented to the United States in stark terms:

> []China, from a counterintelligence perspective, in many ways represents the broadest, most challenging, most significant threat we face as a country. And I say that because for them it is a whole of state effort. It is economic espionage as well as traditional espionage; it is nontraditional collectors as well as traditional intelligence operatives; it's human sources as well as cyber means…the volume of it, the pervasiveness of it, the significance of it, is something I think this country cannot underestimate.[11]

In August 2018, the Department of Defense ("DoD") echoed the FBI Director's assessment by warning in a report to Congress that "China uses its cyber capabilities to support intelligence collection against U.S….defense industrial base sectors."[12] According to the DoD report, the access and skill seen in past Chinese intrusions "are similar to those necessary to conduct cyber operations in an attempt to deter, delay, disrupt and degrade DoD operations prior to or during a conflict."[13] DHS has similarly warned that "[n]ation-state actors such as China…have used cyber intrusions to steal private sector proprietary information and sabotage military and critical infrastructure. [ ] China will continue to use cyber espionage and bolster cyber-attack capabilities to support its national security priorities."[14]

---

[9] *Id.*

[10] *Worldwide Threat Assessment of the U.S. Intelligence Community Before the S. Select Comm. On Intelligence*, 116th Cong. 5 (2019) (statement of Daniel R. Coats, Director of National Intelligence) (hereinafter 2019 ODNI Threat Assessment), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

[11] Tara Chan, *FBI director calls China 'the broadest, most significant' threat to the US and says its espionage is active in all 50 states***,** Business Insider, Jul. 19, 2018, https://www.businessinsider.com/fbi-director-says-china-is-the-broadest-most-significant-threat-to-the-us-2018-7 (remarks delivered at the Aspen Security Forum).

[12] Office of the Sec'y of Def. Ann. Rep. to Cong., *Military and Security Developments Involving the People's Republic of China 2018*, at 75 (May 16, 2018), https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF.

[13] *Id*.

[14] *China's Non-traditional Espionage Against the United States: The Threat and Potential Policy Responses: Hearing Before the S. Comm. on the Judiciary*, 115th Cong., at 1 (Dec. 12,

In September 2018, the White House released its National Cyber Strategy, a comprehensive outline of "how the United States will ensure the American people continue to reap the benefits of a secure cyberspace that reflects our principles, protects our security, and promotes our prosperity."[15] Within the prescribed strategy, the Administration recognized that "the United States is engaged in a continuous competition against strategic adversaries [such as China], rogue states, and terrorist and criminal networks….These adversaries use cyber tools to undermine our economy and democracy, steal our intellectual property, and sow discord in our democratic processes."[16] In addition, the strategy highlighted the economic damage resulting from cyber intrusions, estimating that "China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft."[17]

In November 2018, the Director of the FBI again warned that "no country poses a broader, more severe intelligence collection threat than China. [ ] Nearly every FBI field office currently has economic espionage cases that lead back to China….They're using an expanding set of nontraditional methods to do that—both lawful and unlawful—from things like foreign investments and corporate acquisitions, to cyber intrusions and supply chain threats."[18]

The FBI Director was not alone in bringing public attention to the Chinese government's activities. The alarm was also sounded by the Office of the U.S. Trade Representative ("USTR"), which reported in its March 2018 Section 301 Report that "cyber theft [was] one of China's preferred methods of collecting commercial information because of its…plausible deniability."[19] In its November 2018 Update to its Section 301 findings, the USTR stated that incidents of Chinese cyber thefts were rapidly accelerating.[20]

These repeated warnings by the U.S. Intelligence Community and other agencies are supported by a number of public law enforcement actions against Chinese actors. DOJ's

---

2018) (statement of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security).

[15] *National Cyber Strategy of the United States of America*, White House, at 2 (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[16] *Id.*

[17] *National Cyber Strategy of the United States of America*, White House, at 2 (Sept. 2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

[18] Christopher Wray, Dir. Fed. Bureau of Investigation, Address at the Ninth Annual Financial Crimes and Cybersecurity Symposium, Keeping our Financial Systems Secure: a Whole-of-Society Approach, at 2 (Nov. 1, 2018), (transcript available at https://www.fbi.gov/news/speeches/keeping-our-financial-systems-secure-a-whole-of-society-response).

[19] Office of the U.S. Trade Representative, *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 153 (Mar. 22, 2018), https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF (hereinafter 301 Report).

[20] Office of the U.S. Trade Representative, *Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, at 10-22 (Nov. 20, 2018), https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf.

charging documents continue to expose the People's Republic of China ("PRC") government's nefarious pattern of economic espionage and trade secrets theft. Specifically, about 80 percent of economic espionage cases (which allege trade secret theft intended to benefit a foreign state) implicate the Chinese state (as opposed to another country), and about two-thirds of DOJ's trade secrets cases overall have some nexus to China. Going back to December 20, 2018, DOJ indicted two defendants for working in association with a Chinese intelligence service to hack into managed service providers ("MSP") here and abroad for the purpose of stealing, among other data, intellectual property and confidential business and technological information of MSP clients in the banking and finance, telecommunications and consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining sectors. In 2019 alone, DOJ secured seven convictions or guilty pleas in economic and traditional espionage cases related to China. And in July of this year, for example, DOJ announced an indictment against two Chinese hackers for conducting a decade-long hacking campaign to steal U.S. intellectual property and confidential business information, including COVID-19 research, from a variety of industries, including high tech manufacturing, pharmaceuticals, and defense.[21] The conspirators stole terabytes of sensitive data, in some instances for their own personal gain, but in others to benefit the Chinese government's Ministry of State Security ("MSS") and other Chinese government agencies.[22]

Charges such as those demonstrate at a granular level how the Chinese government uses all available levers to steal sensitive U.S. person data, trade secrets, and other commercially valuable information. These cases further reveal the techniques the Chinese government uses in its campaign to steal from, replicate, and replace U.S. companies. The pervasiveness of this cyber-enabled espionage is reflected in the 2019 ODNI Threat Assessment, which warns not only of the PRC government's cyber activities, but also of the potential use of "Chinese information technology firms as *routine and systemic espionage platforms* against the United States and allies."[23] Indeed, as described in great detail in the USTR Section 301 Report, the Chinese government's "military-civil fusion" policy calls for integrating platforms for information sharing and collaboration between, among others, the People's Liberation Army ("PLA") and Chinese enterprises. Moreover, according to the report, "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."[24]

In July 2018, similar warnings were issued by the National Counterintelligence and Security Center ("NCSC"), which stated that "the Chinese government seeks to enhance its collection of U.S. technology by enlisting the support of a broad range of actors spread

---

[21] *See* Press Release, Office of Public Affairs, U.S. Dep't of Justice, Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (July 21, 2020), https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion; *see also United States v. Li Xiaoyu*, No. 4:20-CR-6019-SMJ, Indictment (E.D. Wash. July 7, 2020).

[22] *United States v. Li Xiaoyu*, No. 4:20-CR-6019-SMJ, Indictment at 3.

[23] *See* 2019 ODNI Threat Assessment at 5.

[24] *See* 301 Report, at 164.

throughout its [ ] industrial base."[25] Put simply, the Chinese government uses its firms and companies as extensions of its apparatus. Those concerns are particularly acute with respect to Chinese state-owned enterprises ("SOE") and their subsidiaries, because the Chinese government is able to exercise direct control over those entities. Thus, the same national security and law enforcement concerns the Executive Branch raised in the China Telecom[26] and China Mobile International (USA), Inc. ("China Mobile")[27] recommendations apply equally to the Companies.

The Chinese government's majority ownership and control of the Companies through CITIC, combined with Chinese intelligence and cybersecurity laws, raise significant concerns that the Companies will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests. The PRC's 2017 Cybersecurity Law and its 2017 National Intelligence Law, in particular, impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for Beijing's intelligence gathering activities.[28] Other provisions, such as those contained in the 2019 Cryptography Law, impose requirements that will expose commercial encryption used within China to testing and certification by the Chinese government, potentially facilitating those same intelligence activities.[29]

The 2017 Intelligence Law provides Chinese government's intelligence services with greater powers to compel Chinese citizens and organizations "to cooperate, assist, and support Chinese intelligence efforts *wherever they are in the world*."[30] As the Commission noted in its 2019 *China Mobile* Order:

---

[25] *Foreign Economic Espionage in Cyberspace*, National Counterintelligence and Security Center 5 (July 26, 2018), https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace.

[26] *See* Exec. Branch Recommendation to Revoke China Telecom.

[27] *See Redacted Executive Branch Recommendation to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization*, FCC No. ITC-214-20110901-00289, at 6-7 (filed July 2, 2018) (hereinafter "Exec. Branch Recommendation to Deny China Mobile"), https://licensing.fcc.gov/myibfs/download.do?attachment_key=1444739.

[28] *Subcommittee on Crime and Terrorism, Committee on the Judiciary, United States Senate Hearing, Dangerous Partners: Big Tech and Beijing*, 116th Congress (2019-2020), March 4, 2020 (statement of Deputy Assistant Attorney General Adam S. Hickey, National Security Division, U.S. Department of Justice) (hereinafter "A. Hickey Statement") https://www.judiciary.senate.gov/meetings/dangerous-partners-big-tech-and-beijing.

[29] *See* A. Hickey Statement.

[30] *See* China Mobile Order, 34 FCC Rcd 3361 (4) at 5 ¶ 17 (emphasis added); *see also* Carolina Dackö and Lucas Jonsson, *Applicability of National Intelligence Law to Chinese and non-Chinese Entities,* Mannheimer Swartling (Jan. 2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf; *see also National Intelligence Law of the People's Republic,* National People's Congress, (last visited Mar. 24, 2020), https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (Google's cache of http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529.htm).

> Article 7 of the 2017 National Intelligence Law provides "an 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." 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.[31]

Additionally, the Cybersecurity Law of the People's Republic of China, and the implementing regulation for the Cybersecurity Law, impose more specific obligations for telecommunications systems operators, even if they are not state owned. For example, the June 1, 2017 Cybersecurity Law requires extensive cooperation by telecom and network operators. Article 28 of the Cybersecurity Law states that "[n]etwork operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[32] "Network operators" are broadly defined as "network owners, network managers, and network service providers."[33] This vague definition ensnares both foreign and Chinese network operators that own or manage a network or provide online services anywhere within China.[34] Article 49 further states that "Network operators shall cooperate with cybersecurity and information departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law."[35]

The consequences of this 2017 Cybersecurity Law are clarified in the implementing regulation, the November 1, 2018 "Regulation on Internet Security Supervision by Public Security Organs" (Order No. 151 of the Ministry of Public Security).[36] The regulation authorizes

---

[31] China Mobile Order, 34 FCC Rcd 3361 (4) at 5 ¶ 17 n.55.

[32] Rogier Creemers, Paul Triolo, and Graham Webster, *Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)*, New America (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

[33] *Id.* (2017 Cybersecurity Law, Article 76(3), providing definition of "network operators").

[34] *Id.* (2017 Cybersecurity Law, Article 2); *see also*, *White Paper: Implementing China's Cybersecurity Law,* Jones Day (Aug. 2017), https://www.jonesday.com/en/insights/2017/08/implementing-chinas-cybersecurity-law.

[35] Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/; 中华人民共和国网络安全法, National People's Congress, http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm (last visited Feb. 21, 2019) (official Chinese text).

[36] *See China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*, Library of Congress (Nov. 13, 2018), https://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-inspection-powers-issued/; *see also*, *China's New Cybersecurity Measures Allow State Policy to Remotely Access Company Systems*, Recorded Future Blog (Feb. 8, 2019), https://www.recordedfuture.com/china-

the Ministry of Public Security to conduct on-site and remote inspections of any company with five or more networked computers, to copy user information, log security response plans during on-site inspections, and check for vulnerabilities.[37] The People's Armed Police would also be present at inspections to ensure compliance with the inspection.[38] For remote inspections, the Ministry of Public Security would be permitted to use certain cybersecurity service agencies.[39]

Both the 2017 Cybersecurity Law and 2018 Regulation on Internet Security Supervision provide little, if any, detail about the available legal procedures or judicial oversight to challenge any Chinese government requests. According to industry sources, these new laws codified existing practices rather than imposing wholly new obligations.[40] The Companies' ultimate parent, as a state-owned entity, is subject to these Chinese cyber and national security laws.

Much like the national security environment, the Companies are not the same providers today that they were when they executed the Letter of Assurance. In March 2009, Pacific Networks stated that the pending authorization would authorize international resold services to all international points, and that ComNet held an authorization to provide international telecommunications services.[41] ComNet also provided international direct dial and wholesale prepaid calling card services.[42] Today, the Companies provide additional services that were not contemplated at the time of the Letter of Assurance, including cloud-based Voice over Internet Protocol ("VoIP") service to small and medium-size enterprise customers and website development and hosting services.[43] Similar to China Mobile's anticipated customers, the Companies' customers also include fixed and mobile network operators, wholesale carriers, and calling card customers.[44] The Executive Branch judged that the Chinese government could exploit China Mobile's interconnections and access to U.S. companies and data.[45] The Companies' similar interconnections and customers present the same opportunity for exploitation by the Chinese government, including the ability to conduct or to increase economic espionage and collect intelligence against the United States.[46]

---

cybersecurity-measures/; 公安机关互联网安全监督检查规定（公安部令第151号), https://www.mps.gov.cn/n2254314/n2254409/n4904353/c6263180/content.html (last visited Mar. 4, 2019).

[37] China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems, Recorded Future Blog, https:/ /www.recordedfuture.com/chinacybersecurity-measures/ (Feb. 8, 2019).

[38] *Id.*

[39] *Id.*

[40] Covington & Burling LLP, *China Releases New Regulation on Cybersecurity Inspection*, Inside Privacy (Oct. 23, 2018), https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/.

[41] Response to Order to Show Cause, 4.

[42] *Id.*

[43] *Id.* DOJ recognizes that a Section 214 authorization is not required to offer these services, but the Companies' expanded suite of services now available was not contemplated at the time of this authorization.

[44] *Id.*, 13-15. *See also* Exec. Branch Recommendation to Deny China Mobile;

[45] *See* Exec. Branch Recommendation to Deny China Mobile, 15.

[46] *Cf. Id.*

As noted above, the U.S. government has in the past several years escalated its warnings about the threats posed by Chinese government-sponsored cyber actors in the current national security environment. These warnings are not limited to direct acts by only the Chinese government itself, but also include its potential use of Chinese information technology firms as routine and systemic espionage platforms against the United States.[47] Multiple agencies in the Executive Branch have also initiated, separately and collectively, a widespread effort to protect the nation's communications networks from potential security threats. In November 2018, DHS convened the Information and Communications Technology Supply Chain Risk Management Task Force (ICT SCRM Task Force), a public-private partnership formed to examine and develop consensus recommendations to identify and manage risk to the global information and communications technology supply chain.[48] In November 2018, DOJ announced the roll-out of its China Initiative, bringing its resources and focus to address the ongoing threat to our national security posed by China's economic espionage and other forms of economic aggression.[49] In addition to identifying and prosecuting those engaged in trade secret theft, hacking, and economic espionage, DOJ has prioritized protecting U.S. critical infrastructure against external threats through foreign direct investment and supply chain compromises, as well as combatting covert efforts to influence the American public and policymakers without proper transparency.[50]

On May 15, 2019, the President signed the Executive Order on Securing the Information and Communications Technology and Services Supply Chain (E.O. 13873), which declares a

---

[47] *See* 2019 ODNI Threat Assessment, at 5.

[48] Department of Homeland Security, Press Release, *CISA ICT Supply Chain Risk Management Task Force Launches Work Streams* (Feb. 26, 2019), https://www.cisa.gov/cisa/news/2019/02/26/cisa-s-ict-supply-chain-risk-management-task-force-launches-work-streams.

[49] Department of Justice, Press Release, *Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage*, Nov. 1, 2018, https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage.

[50] *See* Letter from William P. Barr, Attorney General, to Ajit Pai, Chairman, Federal Communications Commission, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al. (Nov. 13, 2019) (hereinafter "Barr Letter") (supporting the FCC's draft Report and Order concerning national security threats to the communications supply chain, particularly the proposed designation of Huawei and ZTE as covered companies for purposes of that rule); *see also* Department of Justice, Press Release, *Attorney General William P. Barr Delivers the Keynote Address at the Department of Justice's China Initiative Conference*, Feb. 6, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-department-justices-china ("The department confronts these threats through the Committee on Foreign Investment in the United States and Team Telecom . . . earlier this year, based on a recommendation from Justice and other agencies, the Federal Communications Commission denied a license to China Mobile on national security grounds."); Department of Justice, Press Release, *Attorney General William P. Barr Delivers Remarks on China Policy at the Gerald R. Ford Presidential* Museum, July 16, 2020, https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-china-policy-gerald-r-ford-presidential ("I have previously spoken at length about the grave risks of allowing the world's most powerful dictatorship to build the next generation of global telecommunications networks, known as 5G.".

national emergency with respect to the unrestricted acquisition or use of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries.[51] Invoking authority under the International Emergency Economic Powers Act[52] and consistent with the National Emergencies Act,[53] E.O. 13873 prohibits "any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States" for certain covered transactions. The Executive Order applies to transactions that: (1) involve information and communications technology of persons with a nexus to a "foreign adversary"; and (2) pose an undue risk to U.S. telecommunications technology and infrastructure or national security.

The Companies, as international Section 214 authorization holders, are connected to the domestic telecommunications networks of the United States and have direct access to the telephone lines, fiber-optic cables, cellular networks, and communication satellites that constitute those networks. Such connections and access can provide a strategic capability to target, collect, alter, block, and re-route network traffic. This ability is detrimental to the monitoring of network facility security, the need to work with service providers to identify and disrupt unlawful activities such as computer intrusions, and the need for assistance from trusted service providers when investigating past and current unlawful conduct. Allowing a sophisticated and determined threat actor such as the PRC government to have access and control over large-scale telecommunications entities with FCC authorization to provide international telecommunications services within the United States would be undeniably disruptive to each of these activities. The PRC government could use the Companies' 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. Moreover, the PRC government, through the Companies, would have a greater ability to monitor, degrade, and disrupt U.S. government communications. In addition, due to least-cost routing, the communications of U.S. government agencies to any international destinations may conceivably pass through the Companies' network during transit, even if the agencies are not actual customers of the Companies.

Although the Monitoring Agencies have not identified acts of non-compliance under the minimal conditions placed on the Companies' Section 214 authorizations, the Letter of Assurance only accounts for the security risks as they existed more than a decade ago that corresponded to nominal notification and certain information storage requirements.[54] As noted above, the national security environment has evolved since those conditions were put in place in 2009 while the Companies' oversight restrictions have not. Important here, the Chinese government's ownership and control over the Companies undermines the Monitoring Agencies confidence that additional mitigation measures would effectively address the evolved law

---

[51] Exec. Order No. 13873, *Securing the Information and Communications Technology and Services Supply Chain*, 84 FR 22689-22692 (May 15, 2019).

[52] 50 U.S.C. 1701 *et seq.*

[53] 50 U.S.C. 1601 *et seq.*

[54] *See* Response to Order to Show Cause, 4-5 (listing the Companies' obligations under the Letter of Assurance).

enforcement and national security risks.[55] Put simply, mitigation requires a minimum level of trust, and that level of trust is absent here.[56]

That notion is consistent with and reflected in other recent matters that have come before the FCC. Attorney General Barr stated last year that untrusted entities in the telecommunications network places these networks at risk.[57] Untrusted telecommunications providers can facilitate espionage or disrupt critical infrastructure at the request of a foreign power.[58] The PSI Report stated that state ownership of a telecommunications provider does not presume a national security risk.[59] However, the Senate also determined that the national security concerns Team Telecom and the FCC outlined in relation to China Mobile are applicable to other carriers operating in the United States, including the Companies.[60] So long as the Companies control their network, the traffic transmitting this network remains subject to exploitation, influence, and control by the Chinese government.[61] The Executive Branch relies on parties to mitigation agreements to adhere to mitigation agreement provisions, and self-report any problems or issues of non-compliance. The Chinese government's ultimate ownership over the Companies means that the Monitoring Agencies cannot rely on the Companies to self-report violations of more aggressive mitigation measures, especially if the Chinese government were to direct the Companies to violate those terms.[62]

Chairman Pai stated last year that China Mobile, a Chinese state-owned entity, is vulnerable to exploitation, influence, and control by the Chinese government.[63] He further noted that the Chinese government's ongoing involvement in computer intrusions and economic espionage create a significant risk that the Chinese government would use China Mobile to threaten U.S. national security, law enforcement, and economic interests.[64] Pacific Networks and ComNet are ultimately owned and controlled by CITIC, a Chinese state-owned entity, and the

---

[55] *See generally* China Mobile Order *and* Exec. Branch Recommendation to Revoke China Telecom.

[56] *See* e.g., Exec. Branch Recommendation to Deny China Mobile, 16-17; Exec. Branch Recommendation to Revoke China Telecom; *and Exec. Branch Recommendation for a Partial Denial and Partial Grant of the Application for a Submarine Cable Landing License for the Pacific Light Cable Network,* File No. SCL-LIC-20170421-00012; SCL-AMD-20171227-00025; SCL-STA-20180907-000333, et. al. (filed Jun 17, 2020) ("Exec. Branch Recommendation to Deny in Part PLCN").

[57] *See Barr Letter,* 2.

[58] *Id.*

[59] *See* PSI Report, 5.

[60] *Id.*

[61] *Cf.* Exec. Branch Recommendation Deny China Mobile*,* 16-17.

[62] *Cf. Id.*

[63] *See* China Mobile Order, 34 FCC Rcd 3361 (4), App. A, Statement of Chairman Ajit Pai.

[64] *Id.*

Companies' continued operations within the United States present these same concerns. We support the Commission's continued efforts to protect and secure our nation's telecommunications infrastructure.

Respectfully submitted,

Kathy Smith
Chief Counsel

cc:

Loyaan Egal
Deputy Chief for Telecommunications
Foreign Investment Review Section
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
loyaan.egal@usdoj.gov

Alice Suh Jou
Attorney
Foreign Investment Review Section
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530
alice.s.jou2@usdoj.gov

Milton Brown
Deputy Chief Counsel
National Telecommunications and Information Administration
U.S. Department of Commerce, Room 4713
14th Street and Constitution Avenue NW
Washington, D.C. 20230
mbrown@ntia.gov

Jeffrey J. Carlisle
Counsel to Pacific Networks Corp. and ComNet (USA) LLC
Lerman Senter PLLC
2001 L Street NW, Suite 400
Washington, DC 20036
jcarlisle@lermansenter.com

Stephen Coran
Counsel to Pacific Networks Corp. and ComNet (USA) LLC
Lerman Senter PLLC
2001 L Street NW, Suite 400
Washington, DC 20036
scoran@lermansenter.com

Rebecca Jacobs Goldman
Counsel to Pacific Networks Corp. and ComNet (USA) LLC
Lerman Senter PLLC
2001 L Street NW, Suite 400
Washington, DC 20036
rgoldman@lermansenter.com

David Burns
Counsel to Pacific Networks Corp. and ComNet (USA) LLC
Lerman Senter PLLC
2001 L Street NW, Suite 400
Washington, DC 20036
dburns@lermansenter.com

Jonathan Garvin
Counsel to Pacific Networks Corp. and ComNet (USA) LLC
Lerman Senter PLLC
2001 L Street NW, Suite 400
Washington, DC 20036
jgarvin@lermansenter.com

Linda Peng
General Manager, HRA & Admin
ComNet (USA) LLC
100 N. Barranca Street, Suite 910
West Covina, CA 91791
lindapeng@comnet-telecom.com