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

In the Matter of	)	
	)	
Pacific Networks Corp. and	)	GN Docket No. 20-111;
ComNet (USA) LLC	)	ITC-214-20090105-00006;
	)	ITC-214-20090424-00199
	)	

ORDER INSTITUTING PROCEEDING ON REVOCATION AND TERMINATION

Adopted: March 17, 2021 **Released: March 19, 2021**

By the Commission: Acting Chairwoman Rosenworcel and Commissioner Starks issuing separate statements.

TABLE OF CONTENTS

I. INTRODUCTION

1. In this Order, we institute a proceeding to revoke the domestic authority and revoke and/or terminate the international authorizations issued to Pacific Networks Corp. (Pacific Networks) and its wholly owned subsidiary, ComNet (USA) LLC (ComNet), pursuant to section 214 of the Communications Act of 1934, as amended (Act).[1] We find that Pacific Networks and ComNet have

[1] 47 U.S.C. § 214; *Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, Order to Show Cause, 35 FCC Rcd 3733 (IB, WCB, EB 2020) (*Order* (continued….)

failed at this stage to dispel serious concerns regarding their retention of section 214 authority in the United States.[2] Pacific Networks and ComNet have also failed to fully respond to the questions presented in the *Order to Show Cause*. We adopt procedures that will allow for Pacific Networks and ComNet, interested Executive Branch agencies,[3] and the public to present further arguments or evidence in this matter. As such, Pacific Networks and ComNet will have forty (40) days to answer the questions in Appendix A and present arguments and evidence. We then provide the public and the Executive Branch agencies with forty (40) days to respond to Pacific Networks' and ComNet's reply. Pacific Networks and ComNet will then have twenty (20) days to present any additional evidence or arguments demonstrating why the Commission should not revoke and/or terminate their section 214 authorities.

II. BACKGROUND

2. Congress created the Commission, among other reasons, "for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications . . . ."[4] Promotion of national security is an integral part of the Commission's public interest responsibility, including its administration of section 214 of the Act,[5] and indeed one of the core purposes for which Congress created the Commission.[6] The Commission has taken a number of targeted

(Continued from previous page)
to Show Cause); Pacific Networks Corp. and ComNet (USA) LLC, Response to Order to Show Cause, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199 (June 1, 2020) (Pacific Networks and ComNet Response) (filing with the Commission a public filing and a non-public business confidential filing).

[2] *See China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order Instituting Proceedings on Revocation and Termination and Memorandum Opinion and Order, 35 FCC Rcd 15006, 15006-07, paras. 1-2 (2020) (*China Telecom Americas Order Instituting Proceedings*); *Order to Show Cause*, 35 FCC Rcd at 3735-36, para. 6; *China Mobile International (USA) Inc.*; *Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, Memorandum Opinion and Order, 34 FCC Rcd 3361, 3363-64, 3365-66, 3369-70, paras. 3, 8, 17-18 (2019) (*China Mobile USA Order*).

[3] For purposes of this Order, we refer to the following agencies collectively as "Executive Branch agencies": Department of Justice (DOJ), Department of Homeland Security (DHS), Department of Defense (DOD), 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. This list represents a different subset of U.S. government agencies than those that are members of or advisors to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee). *See* Executive Order No. 13913 of April 4, 2020, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643 (Apr. 8, 2020) (Executive Order 13913); *see also* Letter from Kathy Smith, Chief Counsel, National Telecommunications and Information Administration, U.S. Department of Commerce, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau at 1 (Nov. 16, 2020) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199) (Executive Branch Letter). DOJ, DHS, and DOD also are known informally as "Team Telecom."

[4] 47 U.S.C. § 151.

[5] *See 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*, *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market*, IB Docket 97-142, Order on Reconsideration, 15 FCC Rcd 18158 (2000) (*Reconsideration Order*).

[6] *See Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11436, para. 34 (2019) (*Protecting Against National Security Threats Order*), *appeal pending in Huawei Technologies USA v. FCC*, No. 19-60896 (5th Cir.); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second (continued….)

steps to protect the nation's communications infrastructure from potential security threats,[7] and we continue to do so here.

A. Revocation of Domestic and International Section 214 Authority

3. Section 214(a) of the Act prohibits any carrier from constructing, extending, acquiring, or operating any line, and from engaging in transmission through any such line, without first obtaining a certificate from the Commission "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 . . . ."[8] In 1999, the Commission granted all telecommunications carriers blanket authority under section 214 of the Act to provide domestic interstate services and to construct or operate any domestic transmission line.[9] In doing so, the Commission found that the "present and future public convenience and necessity require the construction and operation of all domestic new lines pursuant to blanket authority," subject to the Commission's ability to revoke a carrier's section 214 authority when warranted to protect the public interest.[10] The Commission similarly considers the public interest to determine whether revocation of an international section 214 authorization is warranted. For example, in the *Foreign Participation Order* and the *Reconsideration Order*, the Commission delineated a non-exhaustive list of circumstances where it reserved the right to designate for revocation an international section 214 authorization based on public interest considerations.[11] The Commission has initiated revocation proceedings concerning section 214 authorizations in different contexts.[12]

(Continued from previous page)
Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7822, para. 5 (2020) (*Protecting Against National Security Threats Declaratory Ruling and Second Further Notice*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Second Report and Order, 35 FCC Rcd 14284, 14285, para. 2 (2020) (*Protecting Against National Security Threats Second Report and Order*); *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15007, para. 2.

[7] *See, e.g.*, *China Mobile USA Order,* 34 FCC Rcd at 3365-66, 3376-77, 3380, paras. 8, 31-32, 38; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, paras. 26-27; *Protecting Against National Security Threats Declaratory Ruling and Second Further Notice*, 35 FCC Rcd at 7821-22, paras. 2-3; *see Protecting Against National Security Threats Second Report and Order*, 35 FCC Rcd at 14285, para. 1; *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15006, para. 1.

[8] 47 U.S.C. § 214(a) (emphasis added). The Supreme Court has determined that the Commission has considerable discretion in deciding how to make its section 214 public interest findings. *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, 40-44, 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); *Streamlining the International Section 214 Authorization Process and Tariff Requirements*, IB Docket No. 95-118, Report and Order, 11 FCC Rcd 12884, 12903, para. 44, n.63 (1996) (*Streamlining Orde*r).

[9] *Implementation of Section 402(b)(2)(A) of the Telecommunications Act of 1996*; *Petition for Forbearance of the Independent Telephone & Telecommunications Alliance*, Report and Order and Second Memorandum Opinion and Order, 14 FCC Rcd 11364, 11365-66, para. 2 (1999) (*Domestic 214 Blanket Authority Order*). The Commission did not extend this blanket authority to international services. *Id.*, at 11365-66, para. 2 & n.8; 47 CFR § 63.01.

[10] *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11374, para. 16. The Commission has explained that it grants blanket section 214 authority, rather than forbearing from application or enforcement of section 214 entirely, in order to remove barriers to entry without relinquishing its ability to protect consumers and the public interest by withdrawing such grants on an individual basis. *Id.* at 11372-73, 11374, paras. 12-14, 16.

[11] *See, e.g.*, *Foreign Participation Order*, 12 FCC Rcd at 24023, para. 295 (where the Commission finds that a U.S. carrier has engaged in anticompetitive conduct); *Reconsideration Order*, 15 FCC Rcd at 18173, para. 28 (where the Commission finds that a U.S. carrier has acquired an affiliation with a foreign WTO carrier and such affiliation
(continued….)

4. As part of the Commission's public interest analysis, the Commission considers a number of factors and examines the totality of the circumstances in each particular situation. One of the factors is whether the application for or retention of the authorization raises any national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's or authorization holder's reportable foreign ownership.[13] With regard to this factor, the Commission has sought the expertise of the relevant Executive Branch agencies for over 20 years, and has accorded deference to their expertise in identifying such a concern.[14] The Commission has formalized the review process for the Executive Branch agencies to complete their review consistent with the President's April 4, 2020 Executive Order No. 13913 that established the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee).[15] The Commission ultimately makes an independent

(Continued from previous page)
poses a very high risk to competition that cannot be remedied by safeguards); *id*. at 18175-76, para. 35 (where the Commission finds that a U.S. carrier has proposed to acquire a controlling interest in a foreign non-WTO carrier that does not satisfy the effective competitive opportunities (ECO) test or the affiliation may otherwise harm the public interest pursuant to the Commission's policies and rules); *see also* 47 CFR § 63.11(g)(2); *Reform of Rules and Policies on Foreign Carrier Entry Into the U.S. Telecommunications Market*, IB Docket No. 12-299, Report and Order, 29 FCC Rcd 4256, 4259, 4266, paras. 6, 22 (2014) (eliminating the ECO test which, among other things, had applied to international section 214 applications filed by foreign carriers or their affiliates that have market power in non-WTO Member countries they seek to serve and to notifications filed by authorized U.S. carriers affiliated with or seeking to become affiliated with a foreign carrier that has market power in a non-WTO Member country that the U.S. carrier is authorized to serve, while continuing to reserve the right to proceed to an authorization revocation hearing if the Commission finds that the affiliation may harm the public interest).

[12] *See, e.g., China Telecom Americas Order Instituting Proceedings*; *CCN, Inc. et al.,* Order to Show Cause and Notice of Opportunity for Hearing, 12 FCC Rcd 8547 (1997) (*1997 CCN, Inc. Order*); *CCN, Inc. et al.,* Order, 13 FCC Rcd 13599 (1998) (revoking a company's operating authority under section 214 for repeatedly slamming consumers); *Rates for Interstate Inmate Calling Services,* Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 14107, 14170, para. 118 (2013); *Lifeline and Link Up Reform and Modernization et al.*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6785, para. 299 (2012); *Kurtis J. Kintzel et al.*; *Resellers of Telecommunications Services,* Order to Show Cause and Notice of Opportunity for Hearing, 22 FCC Rcd 17197, 17197, 17204-05, 17205-07, paras. 1, 22, 24 (2007) (*Kintzel Order*); *Compass, Inc.*; *Apparent Liability for Forfeiture,* Notice of Apparent Liability for Forfeiture and Order, 21 FCC Rcd 15132, 15141-42, para. 29 (2006); *OneLink Communications, Inc., et al.*, Order to Show Cause, 32 FCC Rcd 1884 (EB & WCB 2017).

[13] *See Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66; *Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership*, Report and Order, 35 FCC Rcd 10927, 10963-64, para. 92 (2020) (*Executive Branch Process Reform Report and Order*).

[14] *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66. In the 1997 *Foreign Participation Order*, the Commission affirmed its previously *ad hoc* policy of seeking Executive Branch input 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. In addition to international section 214 authority, the policy also applies to other types of applications with reportable foreign ownership, including applications related to submarine cable landing licenses, assignments or transfers of control of domestic or international section 214 authority, and petitions for declaratory rulings 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 et al.*, IB Docket No. 96-111 et al., Report and Order, 12 FCC Rcd 24094, 24171, paras. 179-80 (1997); *see also Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10928-30, paras. 3-7.

[15] *See generally Executive Branch Process Reform Report and Order*; Executive Order 13913, 85 Fed. Reg. at 19643 (stating that, "[t]he security, integrity, and availability of United States telecommunications networks are vital to United States national security and law enforcement interests"); *id*. at 19643-44 (establishing the "Committee," composed of the Secretary of Defense, the Secretary of Homeland Security, and the Attorney General of the DOJ, who serves as the Chair, and the head of any other executive department or agency, or any Assistant to the President,
(continued….)

decision in light of the information in the record, including any information provided by the applicant, authorization holder, or licensee in response to any filings by the Executive Branch agencies.[16]

B. Pacific Networks' and ComNet's Section 214 Authorities

5. ComNet is a Delaware corporation that is wholly owned by Pacific Networks, also a Delaware corporation.[17] ComNet and Pacific Networks are indirectly and ultimately owned and controlled by the government of the People's Republic of China through a complex series of intermediate holding companies organized in Bermuda, the British Virgin Islands, Hong Kong, and the People's Republic of China that are controlled by CITIC Group Corporation, a Chinese state-owned limited liability company.[18] According to Commission records, the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization, directly owns

(Continued from previous page)
as the President determines appropriate (Members), and also providing for Advisors, including the Secretary of State, the Secretary of Commerce, and the United States Trade Representative).

[16] *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66 ("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.").

[17] *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4. The Commission's records reflect that ComNet, formerly known as CM Tel (USA) LLC, identified itself as a "corporation" on record. *See* Letter from Norman Yuen, Chairman, Pacific Networks Corp., and Fan Wei, Director, CM Tel (USA) LLC, to Stephen Heifetz, Deputy Assistant Secretary for Policy Development, U.S. Department of Homeland Security, and Matthew G. Olsen, Acting Assistant Attorney General, National Security Division, U.S. Department of Justice, at 1 (Mar. 3, 2009) (on file in ITC-214-20090105-00006; ITC-T/C-20080913-00428; ITC-214-20090424-00199) (identifying "Pacific Networks Corp. ('Pacific Networks') and CM Tel (USA) LLC ('CM Tel')" as "both Delaware corporations") (2009 LOA); CM Tel (USA) LLC, Application for Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, for Global Authority to Operate as an International Facilities-Based and Resale Carrier, File No. ITC-214-19990927-00607, Attach. at 4 (filed Sept. 27, 1999) (stating, "CM Tel (USA) LLC is a corporation organized under the laws of the state of Delaware"); *Order to Show Cause*, 35 FCC Rcd at 3734, para. 4 & n.13. We observe, however, in previous filings on record in the International Bureau Filing System (IBFS), that ComNet was identified as a limited liability company, as "ComNet (USA) LLC" (and formerly, CM Tel (USA) LLC). *See, e.g.*, *Order to Show Cause*, 35 FCC Rcd at 3733, 3740-45, n.1, Appx. A; Pacific Networks and ComNet Response at i, 1, 3. We direct ComNet to clarify whether ComNet is a corporation or a limited liability company in its response to this Order. *See* Appx. A.

[18] Pacific Networks and ComNet Response at 10, 33-34, Exh. A; *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4.

100% of CITIC Group Corporation.[19] Other publicly available information, however, indicates that CITIC Group Corporation is funded and owned by China's Ministry of Finance.[20]

6. Pacific Networks and ComNet state that Pacific Networks "provides multi-protocol label switching virtual private networks [(MPLS VPN)] services."[21] Pacific Networks' "MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States and internationally."[22] Pacific Networks and ComNet state that they consider these services to be "within the scope of the services Pacific Networks is authorized to provide under its domestic and international [s]ection 214 authorization."[23] ComNet provides the following services, some of which Pacific Networks and ComNet state are "within the scope of the services ComNet is authorized to provide under its international [s]ection 214 authorization": Wholesale International Direct Dial (IDD) service; Wholesale Short Message Service (SMS); Retail Calling Card Service; Voice over Internet Protocol (VoIP) Service; Website/WeChat Service; and Resale of Mobile SIM Cards.[24]

---

[19] *Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4 & n.15; Pacific Networks Corp., Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20120126-00031, Attach. 1, Exh. A (filed Jan. 26, 2012) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the government entity that "[d]irectly owns 100% of [CITIC Group Corporation]"); ComNet (USA) LLC, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20120126-00030, Attach. 1, Exh. A (filed Jan. 26, 2012) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the government entity that "[d]irectly owns 100% of [CITIC Group Corporation]"). *See also* CITIC Telecom International CPC (USA) LLC, Application for International Section 214 Authority, File No. ITC-214-20120629-00171, Attach. 2 at 6 (filed June 29, 2012) (application withdrawn on June 15, 2020) (identifying "Assets Supervision and Administration Commission of the State Council of China" as the government entity that "[o]wns 100% of CITIC Group Corporation") (CITIC Telecom International CPC (USA) LLC Application for International Section 214 Authority); *id.*, Supplement at 7 (filed Apr. 22, 2015) (identifying "Ministry of Finance of the People's Republic of China of the State Council" as the government entity that "[o]wns 100% of CITIC Group Corporation").

[20] *See* CITIC Group Corporation, *About CITIC: Corporate Governance and Risk Management*, https://www.group.citic/en/About_CITIC/Governance_Risk/ (last visited Mar. 16, 2021) ("CITIC Group . . . is a conglomerate established upon the approval of the State Council. It is funded by the Ministry of Finance on behalf of the State Council."); CITIC Limited, *About Us: History*, https://www.citic.com/en/aboutus/history/ (last visited Feb. 13, 2021) ("In December 2011, CITIC Limited was incorporated as a joint stock limited company in China, 100% owned by CITIC Group Corporation which itself is owned by the Ministry of Finance."); CITIC Group Corporation, 2018 U.S. Resolution Plan (Public Section) at 7, https://www fdic.gov/regulations/reform/resplans /plans/chinacitic-165-1812.pdf ("On behalf of the State Council, the Ministry of Finance of the [People's Republic of China] took the responsibilities of investor and is the sole shareholder of CITIC Group."). Given the discrepancy, we direct Pacific Networks and ComNet to clarify this ambiguity in their response to this Order. *See* Appx. A.

[21] Pacific Networks and ComNet Response at 12.

[22] *Id.* According to Pacific Networks and ComNet, "Pacific Networks does not provide the international circuits required for international MPLS VPN," as those facilities "are purchased from unaffiliated international carriers by Pacific Networks' wholesale customer . . . and then interconnected with Pacific Networks' VPN platform in the United States." *Id.* Pacific Networks and ComNet state that "Pacific Networks purchases from U.S. telecommunications carriers high-speed data connections to customer locations to facilitate provision of the service." *Id.* at 12-13.

[23] *Id*. Pacific Networks and ComNet note that they "reserve and in no way waive the argument that the MPLS VPN services provided by Pacific Networks may not, in fact, require a [s]ection 214 authorization." *Id*. at 13, n.33.

[24] *Id.* at 13-15. Pacific Networks and ComNet state that ComNet's Wholesale IDD Service and Retail Calling Card Service are services that "ComNet is authorized to provide under its international [s]ection 214 authorization." *Id.* at 13-14.

7. Pacific Networks and ComNet each hold an international section 214 authorization.[25] Pacific Networks' authorization is ITC-214-20090105-00006 and ComNet's authorization is ITC-214-20090424-00199. These international section 214 authorizations are conditioned upon Pacific Networks and CM Tel (USA) LLC (renamed ComNet in 2010)[26] abiding by the commitments and undertakings set forth in their March 3, 2009 letter of assurances (LOA) to DHS and DOJ (2009 LOA).[27] Additionally, Pacific Networks and ComNet are authorized to provide domestic interstate telecommunications service pursuant to blanket section 214 authority that the Commission has issued by rule.[28]

8. On April 24, 2020, the International Bureau, Wireline Competition Bureau, and Enforcement Bureau (the Bureaus) issued the *Order to Show Cause* directing Pacific Networks and ComNet to file a response within thirty (30) calendar days demonstrating why the Commission should not initiate a proceeding to revoke and terminate their domestic and international section 214 authorizations.[29] As support, the *Order to Show Cause* referenced the Commission's 2019 *China Mobile USA Order*, in which the Commission denied the section 214 application of China Mobile International (USA) Inc. (China Mobile USA) to provide international telecommunications services between the United States and foreign destinations.[30] In that Order, the Commission found that due to its status as a subsidiary of a Chinese state-owned entity, China Mobile USA is vulnerable to exploitation, influence, and control by the Chinese government.[31] In the *Order to Show Cause*, the Bureaus stated that the Commission's findings in the *China Mobile USA Order* raise questions regarding the vulnerability of authorization holders that are subsidiaries of a Chinese state-owned entity to the exploitation, influence, and control of the Chinese government.[32]

9. The Bureaus stated that such findings also raise questions as to Pacific Networks' and ComNet's ongoing qualifications to hold domestic and international section 214 authorizations, whether retention of these authorizations and ISPC assignments by Pacific Networks and ComNet serves the public convenience and necessity, and whether ComNet's use of its ISPCs is consistent with the purpose

[25] *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2.

[26] *Id.* at 3742, Appx. A, para 4.

[27] *See International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-20090105-00006, Public Notice, 24 FCC Rcd 4155, 4156 (2009) (April 9, 2009 Grant Public Notice); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-20090105-00006, Public Notice, 24 FCC Rcd 6379, 6384 (IB 2009) (Corrections) (April 23, 2009 Grant Public Notice); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-T/C-20080913-00428, Public Notice, 24 FCC Rcd 5376, 5379 (IB 2009) (May 7, 2009 Grant Public Notice).

[28] 47 CFR § 63.01. It is unclear based on the record whether Pacific Networks and ComNet provide domestic interstate services pursuant to their blanket domestic section 214 authority in 47 CFR § 63.01. *See* Pacific Networks and ComNet Response at 12-13, Exh. E. We direct Pacific Networks and ComNet to clarify this in their response to this Order. *See* Appx. A.

[29] *See generally Order to Show Cause*; *see also id.*, 35 FCC Rcd at 3737, 3739, paras. 9, 11. In the *Order to Show Cause*, the Bureaus also asked Pacific Networks and ComNet to explain why the Commission should not reclaim International Signaling Point Codes (ISPCs) provisionally assigned to ComNet. *Id*. at 3737-38, para. 9. Pacific Networks and ComNet provided limited information concerning ComNet's ISPCs and we ask additional questions in Appendix A. *See* Appx. A.

[30] *Order to Show Cause*, 35 FCC Rcd at 3735, para. 5; *see China Mobile USA Order*, 34 FCC Rcd at 3361-62, 3380, paras. 1, 38.

[31] *China Mobile USA Order*, 34 FCC Rcd at 3365-66, para. 8.

[32] *Order to Show Cause*, 35 FCC Rcd at 3735-36, para. 6.

for which they were assigned.[33] Accordingly, the *Order to Show Cause* directed Pacific Networks and ComNet to respond to certain questions concerning their ownership, operations, and other related matters.[34] The Bureaus also directed Pacific Networks and ComNet to explain "whether certain *pro forma* transfer of control actions occurred from 2012 to 2014 concerning the subject international section 214 authorizations and whether Pacific Networks and ComNet appropriately notified the Commission, as required by the Commission's rules,"[35] and to provide "a description of the extent to which Pacific Networks and ComNet are or are not otherwise subject to the exploitation, influence and control of the Chinese government."[36]

10. On June 1, 2020, Pacific Networks and ComNet filed their response to the *Order to Show Cause*, including a public filing and a non-public business confidential filing.[37] Among other arguments, Pacific Networks and ComNet contend that they are not subject to the "'exploitation, influence, and control'" of the Chinese government,[38] and they certify "under penalty of perjury" that neither company has been asked by the Chinese government or the Chinese Communist Party to take action that would jeopardize the national security and law enforcement interests of the United States.[39] Pacific Networks and ComNet further argue that additional mitigation measures could be appropriate to address specific concerns about any security vulnerabilities.[40] To the extent that mitigation is not warranted, Pacific Networks and ComNet request that they be "given an opportunity to respond to the Bureaus' allegations at an evidentiary hearing" before an administrative law judge.[41] Additionally, they argue that the Bureaus, in the *Order to Show Cause*, do not point to specific wrongdoing that would warrant revocation.[42] They contend that adopting "the process the Commission established in the [*China Mobile USA Order*]" in the present circumstances would, in effect, be applying a new requirement for holding section 214 authorizations, and as such, the Commission should only consider the Bureaus' proposed actions through a rulemaking.[43]

11. On October 15, 2020, the International Bureau issued a letter requesting DOJ, on behalf of the Attorney General as Chair of the Committee under Executive Order 13913, to address the

[33] *Id.* at 3736-37, para. 7.

[34] *Id.* at 3737-38, para. 9.

[35] *Id.* at 3738, para. 9; *see also* 47 CFR §§ 63.18, 63.24(f).

[36] *Order to Show Cause*, 35 FCC Rcd at 3738, para. 9.

[37] Pacific Networks and ComNet Response. On May 18, 2020, Pacific Networks and ComNet filed a motion for an extension of the time for their response to the *Order to Show Cause* until June 8, 2020. Pacific Networks Corp. and ComNet (USA) LLC, Motion for Extension of Time, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, at 1, 3-4 (filed May 18, 2020) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199). On May 20, 2020, the International Bureau's Telecommunications and Analysis Division granted Pacific Networks and ComNet an extension of time to respond to June 1, 2020. Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Jeffrey J. Carlisle, Counsel to Pacific Networks Corp. and ComNet (USA) LLC, Lerman Senter PLLC (May 20, 2020), 35 FCC Rcd 5352 (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199).

[38] Pacific Networks and ComNet Response at i, iii, 19, 24-27, 36-37.

[39] *Id.* at 19, 21, 24-25, Declaration of Li Ying (Linda) Peng.

[40] *Id*. at iii, 31-32.

[41] *Id*. at 3.

[42] *Id*. at ii; *see also id.* at 27.

[43] *Id*. at 27-30.

arguments made by Pacific Networks and ComNet in their response to the *Order to Show Cause*.[44] The letter sought "the Committee's views on Pacific Networks and ComNet's arguments concerning whether and how they 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," and asked "the Committee to respond as to whether additional mitigation measures could address any identified concerns."[45]

12. On November 16, 2020, the National Telecommunications and Information Administration (NTIA), on behalf of interested Executive Branch agencies, responded to the International Bureau's October 15, 2020 Letter and provided the views of the interested Executive Branch agencies on whether Pacific Networks and ComNet "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."[46] Among other arguments, the Executive Branch agencies contend that the same national security and law enforcement concerns that the Executive Branch raised in the China Telecom (Americas) Corporation (China Telecom Americas) and China Mobile USA recommendations apply equally to Pacific Networks and ComNet.[47] The Executive Branch agencies assert that the national security environment has changed significantly since 2009—more than a decade ago—and the top threats facing the United States are different now, in view of "the culmination of years of aggressive behavior by the Chinese government and the concomitant counterintelligence challenges confronting the United States."[48] The Executive Branch agencies also state that the Chinese government's ownership and control of Pacific Networks and ComNet through CITIC Group Corporation undermines the Executive Branch agencies' confidence that additional mitigation measures would effectively address the evolved law enforcement and national security risks.[49] The Executive Branch

[44] Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Sanchitha Jayaram, Chief, Foreign Investment Review Section, National Security Division, U.S Department of Justice at 1 (Oct. 15, 2020), 35 FCC Rcd 11493 (October 15, 2020 Letter) (on file in GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199).

[45] *Id*. at 11495.

[46] Executive Branch Letter at 2. For the purposes of the letter, the "interested Executive Branch agencies" include DOJ, DHS, DOD, 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. *Id*. at 1, n.3. The letter "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 [Pacific Networks and ComNet]" due to "the nature of the Commission's request for views on discreet [sic.] factual questions, and the limited time allotted for response." *Id*. at 1.

[47] *Id*. at 6 (citing Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate [China Telecom (Americas) Corporation's] International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (filed Apr. 9, 2020) (Executive Branch Recommendation to Revoke and Terminate) (filing with the Commission a public filing, a non-public business confidential filing, and a classified appendix); Redacted 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 6-7 (filed July 2, 2018) (Executive Branch Recommendation to Deny)); *see also* Executive Branch Recommendation to Revoke and Terminate at 1-3, 41 (describing changed circumstances in the national security environment, including the U.S. government's increased concern in recent years about the Chinese government's malicious cyber activities; stating that operations of a U.S. telecommunications subsidiary of a Chinese state-owned enterprise under the ultimate ownership and control of the Chinese government provide the opportunity for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic).

[48] Executive Branch Letter at 2-3.

[49] *Id*. at 2, 10-12.

agencies also rely on and cite to the June 9, 2020 Senate Permanent Subcommittee on Investigations (Senate Subcommittee) Staff Report titled, "Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers" (PSI Report).[50]

III. DISCUSSION

13. The Bureaus' *Order to Show Cause* directed Pacific Networks and ComNet to show why the Commission should not initiate a proceeding to consider whether to revoke and terminate their domestic and international section 214 authorizations. In this Order, we conclude that Pacific Networks and ComNet have not done so, and thus we initiate a proceeding that we believe is suited to determine whether revocation and/or termination are appropriate.[51] Based on our public interest analysis under section 214 of the Act and the totality of the record evidence, we find that more than sufficient cause exists to initiate further proceedings to determine whether to revoke the domestic section 214 authority and revoke and/or terminate the international section 214 authorizations held by Pacific Networks and ComNet, and we do so herein. To allow Pacific Networks and ComNet to respond to the serious concerns raised in the record as discussed herein, Pacific Networks and ComNet will have a further opportunity to file a written submission to show cause why the *present and future* public interest, convenience, and necessity is served by their retention of their domestic and international section 214 authorities and why the Commission should not revoke their domestic section 214 authority and revoke and/or terminate their international section 214 authorizations. In this regard, we also direct them to respond to certain additional questions set forth below. Following its review of the record, and absent the need for any further information in light of the parties' additional filings, the Commission will determine whether the record as a whole supports revocation and/or termination of Pacific Networks' and ComNet's section 214 authorities.[52]

A. Adequacy of Further Procedures

14. We find that the procedures adopted here are consistent with both principles of due process and applicable law. It is well-established that the Commission's authority to "conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice"[53] includes the authority "to select the personnel and procedures that are best suited to the issues

[50] *Id*. at 2, 11 (citing Staff Report of Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, 116th Congress, *Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers* (June 9, 2020), https://www hsgac.senate.gov/download/threats-to-us-networks-oversight-of-chinese-government-owned-carriers (PSI Report)).

[51] *See* 47 U.S.C. §§ 154(j), 403; 47 CFR § 1.1.

[52] We note that it is now well-established that in the absence of any statutory requirement to the contrary, an administrative hearing is governed by the familiar preponderance of the evidence standard, and not clear and convincing evidence—even in formal administrative hearings required by statute to be conducted on the record. *See* 5 U.S.C. § 556(d) ("[A] sanction may not be imposed . . . except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the reliable, probative, and substantial evidence."); *Steadman v. SEC,* 450 U.S. 91, 101 & n. 21 (1981) (citing *Sea Island Broadcasting v. FCC,* 627 F.2d 240 (D.C. Cir. 1980)); *In re Kay,* 17 FCC Rcd 1834, 1837, para. 11 (2002), *aff'd*, 396 F.3d 1184 (D.C. Cir. 2005). We invite Pacific Networks and ComNet, the Executive Branch agencies, and the public to address this question further in their subsequent filings.

[53] 47 U.S.C. § 154(j); *see FCC v. Schreiber,* 381 U.S. 279, 290 (1965); *FCC v. Pottsville Broadcasting Co.*, 309 U.S. 134, 138 (1940) (holding that "the subordinate questions of procedure in ascertaining the public interest, when the Commission's licensing authority is invoked . . . [are] explicitly and by implication left to the Commission's own devising, so long, of course, as it observes the basic requirements designed for the protection of private as well as public interest" by section 4(j) of the Act); *see also Vermont Yankee Nuclear Power Corp. v. Natural Resources Defense Council, Inc.,* 435 U.S. 519, 524-25 (1978); *id.* at 543-44 (noting the "very basic tenet of administrative law that agencies should be free to fashion their own rules of procedure").

raised in each case and that will achieve a full, fair, and efficient resolution of each hearing proceeding."[54] The Commission has generally relied upon formal hearings before an administrative law judge where the Act requires designation of a matter for hearing under section 309,[55] but it has used other procedures as appropriate for different types of proceedings. For example, the Commission has generally resolved issues on a written record and without an administrative law judge in section 204 tariff proceedings and section 208 complaint proceedings.[56] Even when section 309 applies, the Commission has found it appropriate to proceed on the written record, as when evaluating competing initial cellular applications and in license-renewal and transfer proceedings where the Commission has determined that there are no substantial issues of material fact or credibility issues.[57] In this case, as in the *China Telecom Americas Order Instituting Proceedings*, there is no statutory requirement that any specific procedures be followed, and the basis for instituting these revocation proceedings does not turn on any disputed facts that would benefit from being examined in a hearing before an administrative law judge. Indeed, the Commission has found that "the hearing requirements under Title III applicable to radio applications do not apply to Title II Section 214 applications."[58] Similarly, we do not expect that the question of whether revocation is appropriate will turn on disputed issues of fact, nor will the credibility of any material evidence in the record be reasonably questioned. Rather, we intend here to consider the proper response to facts that are not reasonably disputed, and in particular to the overall national security risks as they figure into our public interest analysis under section 214 of the Act.

15. Pacific Networks and ComNet make various procedural arguments that we reject. Pacific Networks and ComNet request "an opportunity to respond to the Bureaus' allegations at an evidentiary hearing" before an administrative law judge.[59] Pacific Networks and ComNet state that the Commission "consistently has ordered administrative hearings when considering whether to revoke [s]ection 214 authorizations" by "relying on [s]ections 154(i), 214 and 312 of the Act and [s]ection 1.91 of the Commission's rules."[60] But the Commission has never applied its rules under part 1, subpart B[61] to every adjudication.[62] Section 1.91 of the Commission's rules applies subpart B to revocations of "station license[s]" or "construction permit[s]"—terms that refer to spectrum licenses issued under Title III of the

[54] *Procedural Streamlining of Administrative Hearings*, Report and Order, 35 FCC Rcd 10729, 10731, para. 7 (2020).

[55] *See id.* at 10730, para. 3.

[56] *Id.* (citing *July 1, 2018 Annual Access Charge Tariff Filings; South Dakota Network, LLC Tariff F.C.C. No.1*, Memorandum Opinion and Order, 34 FCC Rcd 1525 (2019), and 47 CFR §§ 1.720-.736).

[57] *Id.* at 10730, para. 4 (citing *Inquiry into the Use of the Bands 825-845 MHz and 870-890 MHz for Cellular Communications Systems*, Report and Order, 86 FCC 2d 469 (1981), *Birach Broad. Corp.*, Hearing Designation Order, 33 FCC Rcd 852 (2018), and *Radioactive, LLC*, Hearing Designation Order, 32 FCC Rcd 6392 (2017)). *See also Applications of T-Mobile US, Inc. and Sprint Corp.*, Memorandum Opinion and Order, Declaratory Ruling, and Order of Proposed Modification, 34 FCC Rcd 10578, 10596, para. 42 (2019).

[58] *Application of Oklahoma W. Tel. Co.*, Order, 10 FCC Rcd 2243, 2243-44, para. 6 (1995) (*Oklahoma W. Tel. Co. Order*) (finding no substantial public interest questions existed to justify hearing on Section 214 application) (citing *ITT World Commc'ns v. FCC*, 595 F.2d 897, 900-01 (2d Cir. 1979)).

[59] Pacific Networks and ComNet Response at 3.

[60] *Id.* at 36.

[61] 47 CFR §§ 1.201-.377.

[62] *See Procedural Streamlining of Administrative Hearings*, Notice of Proposed Rulemaking, 34 FCC Rcd 8341, 8343, para. 4 & n.16 (2019) (*Administrative Hearings NPRM*). In fact, section 1.201 of those rules provides that subpart B applies only to cases that "have been designated for hearing." 47 CFR § 1.201. An explanatory note makes clear that the new procedures for written hearings are a subset of such cases. *Id.* note 1.

Act—but, in contrast to an adjacent section of those rules, does not extend to section 214 authorizations.[63] This distinction reflects one in the Act itself, which specifies a procedure for revoking Title III authorizations in section 312,[64] but does not specify any such required procedure for revoking Title II authorizations. Thus, in the recent proceeding updating the Commission's subpart B rules, the Commission noted that "the hearing requirements applicable to Title III radio applications do not apply to Title II section 214 applications."[65]

16. Pacific Networks and ComNet point out five cases between 1997 and 2007 in which the Commission designated for hearing the revocation of section 214 authorizations.[66] Those cases reflect nothing more than the Commission's lawful exercise of its discretion to order a hearing in a particular dispute under section 214.[67] Contrary to Pacific Networks' and ComNet's view, the Commission has never had any established practice of requiring a hearing for all section 214 revocations. Rather, the handful of cases on which Pacific Networks and ComNet seek to selectively rely simply reflect the tailoring of procedures according to the circumstances of each case, under section 4(j), "in such manner as will best conduce to the proper dispatch of business and to the ends of justice."

17. Even if those cases were thought to represent a past policy of applying subpart B to all section 214 revocations, we no longer believe that such a policy is appropriate—and certainly not in cases where the pleadings addressing the relevant national security issues do not identify any need for additional procedures and the public interest warrants prompt response to legitimate concerns raised by the Executive Branch. Instead, in our judgment, the process we outline here is sufficient to resolve the ultimate questions in most section 214 cases while providing carriers with due process.[68] As the Supreme Court has said, "the ordinary principle [is] that something less than an evidentiary hearing is sufficient

[63] 47 CFR § 1.91; *compare id.* § 1.89 (applying to "any person who holds a license, permit[,] *or other authorization*" (emphasis added)). The Act defines "station license" to mean "that instrument of authorization required by this chapter or the rules and regulations of the Commission made pursuant to this chapter, for the use or operation of apparatus for transmission of energy, or communications, or signals by radio, by whatever name the instrument may be designated by the Commission." 47 U.S.C. § 153(49); *see also id*. §§ 307-310, 319. A "construction permit" is "that instrument of authorization required by this chapter or the rules and regulations of the Commission made pursuant to this chapter for the construction of a station, or the installation of apparatus, for the transmission of energy, or communications, or signals by radio, by whatever name the instrument may be designated by the Commission." *Id.* § 153(13). By contrast, telecommunications carriers obtain a "certificate" or an "authorization" under section 214, not a radio "station license or construction permit." *See* 47 U.S.C. § 214 (stating that a carrier must obtain from the Commission "a certificate that the present or future public convenience and necessity require or will require . . ."); 47 CFR §§ 63.01 ("Authority for all domestic common carriers."), 63.21 ("Conditions applicable to all international Section 214 authorizations.").

[64] 47 U.S.C. § 312(c).

[65] *See Administrative Hearings NPRM*, 34 FCC Rcd at 8343, para. 4 & n.16 (internal quotations and alteration omitted).

[66] Pacific Networks and ComNet Response at 36 n.71 (citing *1997 CCN, Inc. Order*, 12 FCC Rcd at 8548; *Publix Network Corp.*, Order to Show Cause and Notice of Opportunity for Hearing, 17 FCC Rcd 11487 (2002); *Business Options, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6881 (2003); *NOS Comm'cns, Inc., et al.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6952 (2003); and *Kintzel Order*). Significantly, none of those matters were ultimately resolved through a hearing under the subpart B rules.

[67] *See Oklahoma W. Tel. Co. Order*, 10 FCC Rcd at 2243, para. 6 (stating that "the Commission has the discretion to designate for evidentiary hearing issues raised in the context of a Section 214 application").

[68] We assume, without deciding, that foreign-owned carriers' interest in retaining section 214 authority to operate communications networks in the United States is entitled to due process protection.

prior to adverse administrative action."[69] Pacific Networks and ComNet state that they "do not waive their right to a hearing prior to any final action by the Commission," [70] but provides no reason to believe that any particular additional process would provide any additional benefit. We find that it suffices in this context to provide a carrier with timely and adequate notice of the reasons for revocation and/or termination; opportunity to respond with its own evidence and to make any factual, legal, or policy arguments; access to all of the unclassified evidence the Commission considers;[71] and a written order from the Commission providing its complete reasoning for any adverse decision. Pacific Networks and ComNet nowhere explain with any specificity what additional process they require or why such process is essential to reaching a fair decision in this matter. So the value of any additional process in preventing erroneous deprivation—one factor in determining what process is due[72]—appears minimal. By contrast, the fiscal and administrative burden of such additional process could be quite substantial and disruptive if it were to involve participation by Commission staff or officials from other agencies in oral proceedings before the Commission.[73] And given the national-security issues at stake, any resulting unwarranted delay could be harmful.[74]

18. The circumstances of this proceeding confirm that additional procedures such as those provided in hearings that are subject to subpart B would serve little purpose here. We intend to base any revocation or termination solely on evidence that has already been introduced or that can be introduced in subsequent written pleadings, most or all of which is already in the possession of or otherwise available to Pacific Networks and ComNet. Nor, based on the current filings, do we see any need for any requests for discovery directed to the Executive Branch agencies that have participated here, because their conduct is not at issue and their filings speak for themselves. Rather, the issues here involve facts within the knowledge or control of Pacific Networks and ComNet.

19. We also conclude at this time that there are no substantial and material questions of fact in this case warranting an evidentiary hearing. The matters under consideration here do not turn on witnesses testifying to their personal knowledge or observations or on individual credibility determinations, for example, but instead on facts that can be fully ascertained through written evidence and on national security and law enforcement concerns associated with Pacific Networks' and ComNet's ultimate ownership and control by the Chinese government. Although we do here direct Pacific Networks and ComNet to provide additional critical information that they should have provided in a complete response to the *Order to Show Cause*, the written record is already substantial, and Pacific Networks and ComNet will have a further opportunity to respond to this Order and to offer any additional evidence or

[69] *Mathews v. Eldridge*, 424 U.S. 319, 343 (1976).

[70] Pacific Networks and ComNet Response at 36; *id* at 3 (stating ". . . should the Commission or the Bureaus elect to move forward with proceedings seeking to revoke the Companies' authorizations and reclaim ComNet's ISPCs, the Companies in no way waive or otherwise wish to forego an evidentiary hearing before an Administrative Law Judge . . . .").

[71] We note that, at this time, no classified evidence has been introduced into the record of this proceeding. If any classified evidence were introduced, we would have authority to protect it from release, 47 U.S.C. § 154(j), and Pacific Networks and ComNet would not be afforded access to it in any case, *see Jifry v. FAA*, 370 F.3d 1174, 1184 (D.C. Cir. 2004).

[72] *Mathews*, 424 U.S. at 335, 344-46.

[73] *Id.* at 347-49.

[74] On the other side of the ledger, private companies have no unqualified right to operate interstate transmission lines—on the contrary, Congress has conditioned such activity on a showing that it would serve the "public convenience and necessity," 47 U.S.C. § 214(a)—and it is especially unlikely that a company owned and controlled by a foreign government can claim to have a substantial right to operate communications networks here in the United States.

arguments.[75] The Commission exercises its well-established discretion[76] to proceed without holding an evidentiary hearing and intends to base its ultimate decision on its overall assessment of the public interest. If, at the conclusion of this process, the Commission is not able to reach a well-founded decision, it could order additional proceedings.

20. We further conclude that, at this time, Pacific Networks and ComNet have shown no need to refer this matter to be considered in the first instance before "an Administrative Law Judge."[77] Even under the subpart B rules, a hearing may be presided over by "an administrative law judge," "one or more Commissioners," or "the Commission" itself.[78] Moreover, if the Commission were to delegate initial responsibility to an administrative law judge (or to one or more Commissioners), the resulting decision could be appealed to the full Commission—which would be required to review the record independently and would not owe any deference to the administrative law judge's determination.[79] Pacific Networks and ComNet have not explained at this stage why the unnecessary extra step of soliciting an intermediate decision from an administrative law judge would enhance the ability of the Commission, which will be the ultimate arbiter in any event, to understand any particular material matter in dispute. Nor have Pacific Networks and ComNet articulated any particularized and compelling reason why the Commission or any individual Commissioner would not be able to serve as a neutral decisionmaker in this matter.

21. Pacific Networks and ComNet also argue that "the Commission limits [s]ection 214 revocation to those instances where there are repeated or willful abuses by companies of their privileges under their authorizations" and therefore "any action to revoke Pacific Networks' or ComNet's [s]ection 214 authorizations would be unwarranted."[80] It would be unreasonable to conclude that serious misconduct could be the only justification for revocation, given the Commission's ongoing responsibility to evaluate all aspects of the public interest, including national security and law enforcement concerns that are "independent of our competition analysis."[81] Indeed, while as noted above section 312 does not apply here, it permits revocation of Title III licenses and permits for a number of other grounds, including "conditions coming to the attention of the Commission which would warrant it in refusing to grant a license or permit on an original application."[82] Finally, we disagree with Pacific Networks' and

[75] Additionally, we note that the Bureaus' *Order to Show Cause* provided Pacific Networks and ComNet with any notice and opportunity that may be required by 5 U.S.C. § 558 before the institution of a proceeding to revoke their authorities, though it appears from the record that "the public . . . interest, or safety" may require revocation in any event. 5 U.S.C. § 558(c). Nothing in the Administrative Procedure Act (APA) requires the application of trial-type procedures to the ensuing proceeding even when section 558 applies. *Empresa Cubana Exportadora de Alimentos Y Productos Varios v. U.S. Dep't of the Treasury*, 638 F.3d 794, 802 (D.C. Cir. 2011) (Kavanaugh, J.) (citing *Gallagher & Ascher Co. v. Simon*, 687 F.2d 1067, 1073-75 (7th Cir. 1982)); *see also China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15015, para 18.

[76] *See NextEra Energy Resources, LLC v. FERC*, 898 F.3d 14, 26 (D.C. Cir. 2018); *Ill. Commerce Comm'n v. FERC*, 721 F.3d 764, 776 (7th Cir. 2013) ("FERC need not conduct an oral hearing if it can adequately resolve factual disputes on the basis of written submissions.").

[77] Pacific Networks and ComNet Response at 3.

[78] 47 CFR § 1.241(a); *cf.* 5 U.S.C. § 556(b) (formal adjudication under the APA may be presided over by an administrative law judge, one or more members of the agency, or the "the agency" itself).

[79] *See Kay v. FCC*, 396 F.3d 1184, 1189 (D.C. Cir. 2005) (explaining that "an agency reviewing an ALJ decision is not in a position analogous to a court of appeals reviewing a case tried to a district court").

[80] Pacific Network and ComNet Response at 19.

[81] *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 65; *see China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15016, para. 19.

[82] 47 U.S.C. § 312(a)(2).

ComNet's argument that the Commission's actions in this case are more appropriately considered through a rulemaking process.[83] It is well established that, "in interpreting and administering its statutory obligations under the Act, the Commission has very broad discretion to decide whether to proceed by adjudication or rulemaking,"[84] and we believe that the issues raised here best lend themselves to resolution through the party-specific procedures that we lay out in this Order.

B. Basis for Revocation of Section 214 Authority

22. When considering the revocation of Pacific Networks' and ComNet's domestic and international section 214 authorities, we consider whether the domestic section 214 authority and international section 214 authorizations continue to serve the public interest, convenience, and necessity, as the Commission found to be the case when it granted blanket domestic section 214 authority to carriers entering the domestic U.S. market and consistent with the inquiry conducted at the time the International Bureau first granted Pacific Networks and ComNet the international section 214 authorizations.[85] Consistent with the recent actions we have taken to secure U.S. telecommunications networks, we institute this further proceeding because of concerns that Pacific Networks' and ComNet's ownership and control by the Chinese government raise significant national security and law enforcement risks with respect to their domestic and international section 214 authority that cannot be addressed through further mitigation with the Executive Branch agencies.[86] In particular, we seek to address concerns that Pacific Networks' and ComNet's ties to the Chinese government—together with Chinese laws obligating Pacific Networks and ComNet and their direct and indirect parent entities and affiliates to cooperate with any request by the Chinese government to use or access their systems—pose a clear and imminent threat to the security of the United States due to Pacific Networks' and ComNet's access to U.S. telecommunications infrastructure.[87]

23. We find that, based on the information available in the record and consistent with the Commission's prior determination regarding risks to U.S. national security and law enforcement interests by a U.S. subsidiary of a Chinese state-owned entity, Pacific Networks and ComNet have not yet adequately demonstrated that they are not susceptible to the exploitation, influence, or control of the Chinese government.[88] Pacific Networks and ComNet failed to fully respond to the questions in the

[83] Pacific Networks and ComNet Response at 27.

[84] *See, e.g.*, *Neustar, Inc. v. FCC*, 857 F.3d 886, 894 (D.C. Cir. 2017) (internal quotation marks and citations omitted); *Chisholm v. FCC*, 538 F.2d 349, 365 (D.C. Cir. 1976) (reiterating that "the choice whether to proceed by rulemaking or adjudication is primarily one for the agency regardless of whether the decision may affect agency policy and have general prospective application") (citing *N.L.R.B. v. Bell Aerospace Co.*, 416 U.S. 267, 291-95 (1974); *SEC v. Chenery Corp.*, 332 U.S. 194, 203 (1947) (stating that "the choice made between proceeding by general rule or by individual, ad hoc litigation is one that lies primarily in the informed discretion of the administrative agency"); *SBC Communications, Inc. v. FCC*, 138 F.3d 410, 421 (D.C. Cir. 1998) (stating that "[i]nherent in an agency's ability to choose adjudication rather than rulemaking. . . is the option to make policy choices in small steps, and only as a case obliges it to") (citation omitted).

[85] *See* 47 U.S.C. § 154(i); § 214 ("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 . . . .") (emphasis added).

[86] *See, e.g.*, 2009 LOA at 10-11.

[87] *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15016-17, para. 20; *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, 11442, paras. 27, 49.

[88] *China Mobile USA Order*, 34 FCC Rcd at 3361-62, 3365-66, 3368-69, paras. 1, 8, 14, 16-17; *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, 11442, paras. 46, 49; *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – Huawei Designation*,

(continued….)

Order to Show Cause and provided minimal, limited, and contradictory statements, which alone could be grounds for revocation, however, based on the record, we find Pacific Networks and ComNet are ultimately owned and controlled by the Chinese government[89] and due to this relationship, Pacific Networks and ComNet may be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight.[90] Further, it appears that Pacific Networks' and ComNet's U.S. operations provide opportunities for Chinese state-sponsored actors to engage in economic espionage, to disrupt and misroute U.S. communications traffic, and to collect intelligence against the United States.[91] The Executive Branch agencies, which have expertise in matters of national security and law enforcement and in monitoring carriers' compliance with risk mitigation agreements, state that "mitigation requires a minimum level of trust, and that level of trust is absent here."[92] We have a longstanding policy of according deference to the Executive Branch agencies' expertise in identifying risks to national security and law enforcement interests.[93] Based on the significant national security and law enforcement concerns raised by the Executive Branch agencies and the evidence in the record, it appears that the public interest requires revocation of Pacific Networks' and ComNet's section 214 authorities.

1. National Security and Law Enforcement Concerns Related to Pacific Networks and ComNet

24. The totality of the evidence in the record presents a serious and compelling case that Pacific Networks' and ComNet's use of their section 214 authorities poses a national security risk and also raises significant law enforcement concerns. The Executive Branch agencies contend that because the Chinese government ultimately owns Pacific Networks and ComNet through CITIC Group Corporation, a Chinese state-owned limited liability company,[94] "there is significant risk the Chinese government would use certain [s]ection 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."[95] The Executive Branch agencies further state that "[t]he Chinese government's majority ownership and control of [Pacific Networks and ComNet] through [CITIC Group Corporation], combined with Chinese intelligence and cybersecurity laws, raise significant concerns that [Pacific Networks and ComNet] will be forced to comply with Chinese government requests, including requests

(Continued from previous page)
Memorandum Opinion and Order, PS Docket No. 19-351, 35 FCC Rcd 14435, 14440-41, paras. 16-17 (2020) (*Huawei Designation Order*).

[89] Pacific Networks and ComNet failed to fully respond to the questions in the *Order to Show Cause* and we therefore direct Pacific Networks and ComNet to respond to the Further Request for Information in Appendix A. *See* Appx. A.

[90] Executive Branch Letter at 6-8; *see also China Mobile USA Order*, 34 FCC Rcd at 3368-69, paras. 14, 16, 17; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, 11442, paras. 46, 49; *Huawei Designation Order*, 35 FCC Rcd at 14440-41, paras. 16-17; *China Telecom Americas Order*, 35 FCC Rcd at 15018, para. 22.

[91] Executive Branch Letter at 8-12; *see also China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15017, 15023-29, paras. 21, 30-36.

[92] Executive Branch Letter at 11.

[93] *See supra* para. 4; *see also China Mobile USA Order*, 34 FCC Rcd at 3362, para. 2; *Huawei Designation Order*, 35 FCC Rcd at 14448, para. 34 & n.117; *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15017, para. 21.

[94] Executive Branch Letter at 2, 11-12; *see also Order to Show Cause*, 35 FCC Rcd at 3734-35, para. 4; Pacific Networks and ComNet Response at 10.

[95] Executive Branch Letter at 2 (citing *China Mobile USA Order*).

for communications intercepts, without the ability to challenge such requests."[96] These laws include the 2017 National Intelligence Law, the 2017 Cybersecurity Law, and the 2019 Cryptography Law.[97] Indeed, the former U.S. National Security Advisor has recently cautioned about "the integrated nature of the Chinese Communist Party's military and economic strategies," noting that the Chinese Communist Party "is obsessed with control—both internally and externally," and that under Article 7 of China's National Intelligence Law, "all Chinese companies must collaborate in gathering intelligence."[98] The PSI Report found, among other things, that "Chinese state-owned companies are subject to an added layer of state influence in that they must comply with strict national security, intelligence, and cyber security laws regardless of where they operate."[99] Based on the record, and in light of the Commission's findings in other related proceedings,[100] we view the arguments of the Executive Branch agencies as persuasive.

25. Pacific Networks' and ComNet's claims about their "factual and legal independence from Chinese government influence"[101] are contradicted by the record and the Commission's findings in other related proceedings.[102] Pacific Networks and ComNet characterize their companies as "small, independently-operated, U.S. domiciled companies that are not wholly-owned by the Chinese government."[103] Pacific Networks and ComNet contend that "[i]n terms of day-to-day management, [they] conduct their operations independently" and "[e]ntities upstream of [Pacific Choice International Limited] are not involved in the daily business or operations of Pacific Networks or ComNet."[104] Pacific Networks and ComNet state that "ComNet's independence is reinforced by the make-up of its employees and leadership. The totality of ComNet's employees are subject to United States laws—either by virtue of full citizenship, their status as a green card holder or in one case an H1-B visa holder. Any employee modifying operations at the direction of foreign influence would expose himself or herself to tremendous personal legal risk."[105] Pacific Networks and ComNet "certify under penalty of perjury" that "Pacific Networks and ComNet are wholly-owned subsidiaries of Pacific Choice International Limited and that company's parent corporation [is] CITIC Telecom International Holdings Limited [(CITIC Tel)]. Executives of their parent corporations do not participate in the daily operations of ComNet or Pacific Networks."[106] Further, they certify that "[t]he extent of the involvement of executives of the parent corporations of Pacific Networks and ComNet is to routinely review the financial positions of Pacific

[96] *Id*. at 6.

[97] *Id*. at 6-8; *see also China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15018, para. 22.

[98] H.R. McMaster, *What China Wants*, The Atlantic, May 2020, at 70, 71, 72-73 (*What China Wants*); *see also* H.R. McMaster, *How China Sees the World: And How We Should See China* (May 2020), https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/.

[99] PSI Report at 9.

[100] *See China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *Protecting Against National Security Threats Order*, 34 FCC Rcd 11423 at 11441, 11442, paras. 46, 49; *Huawei Designation Order*, 35 FCC Rcd at 14440-41, paras. 16-17.

[101] Pacific Networks and ComNet Response at 27.

[102] *See China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *Protecting Against National Security Threats Order*, 34 FCC Rcd 11423 at 11441, 11442, paras. 46, 49; *Huawei Designation Order*, 35 FCC Rcd at 14440-41, paras. 16-17.

[103] Pacific Networks and ComNet Response at 26.

[104] *Id*. at 11.

[105] *Id*. at 25-26.

[106] *Id*., Declaration of Li Ying (Linda) Peng.

Networks and ComNet. These reviews relate only to revenues from and costs of operations, and do not impose any specific obligations with regard to technical or commercial operations."[107]

26. Despite Pacific Networks' and ComNet's claims, the record evidence indicates that ComNet's relationship with its indirect parent entity, CITIC Tel,[108] is not confined to the parent entity "routinely review[ing] the financial positions" as would "any investor."[109] The PSI Report stated that ComNet representatives informed the Senate Subcommittee "that its daily operations are managed by its local management team in California. The representatives, however, acknowledged that [CITIC Tel] reviews the company's budget and U.S. locations."[110] Significantly, the PSI Report stated that "[CITIC Tel] also guides ComNet on its information security policies,"[111] and that "ComNet maintains a company-specific policy, but that policy was drafted based on [CITIC Tel's] guidance."[112] Moreover, the PSI Report stated that "ComNet leverages [CITIC Tel's] network operations center [(NOC)], located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions."[113] Indeed, the record indicates that Pacific Networks and ComNet omitted this and other relevant information in their response to the *Order to Show Cause* concerning the extent of their parent entities' influence and involvement in the companies' operations and decision-making.[114]

27. Further, Pacific Networks' and ComNet's responses to prior inquiries by Team Telecom also indicate that CITIC Tel has oversight of and involvement in ComNet's operations[115]—contrary to the entities' representations in their response to the *Order to Show Cause*. In a December 13, 2017 letter to DOJ, counsel on behalf of Pacific Networks and ComNet enclosed documents, including the "CITIC Telecom IT Security Policy," "CITIC Telecom Password Control Policy Account Lockout Policy," and "CITIC Telecom User Account Policy."[116] The letterhead of these documents are marked {[

[107] *Id*.

[108] *Id*. at 10, Exh. A. Based on the record, CITIC Tel is "a publicly-traded company" that is incorporated and listed in Hong Kong. *See id.* at 10, Exh. A.

[109] *See id.* at 25.

[110] *Id*. at 95 (citing Briefing with ComNet (Apr. 13, 2020)).

[111] *Id*. at 95-96 (citing Briefing with ComNet (Apr. 13, 2020)).

[112] *Id*. at 96 (citing Briefing with ComNet (Apr. 13, 2020)).

[113] *Id*. (citing Briefing with ComNet (Apr. 13, 2020)).

[114] As discussed below, Pacific Networks' and ComNet's representations to the Commission appear to be inconsistent with their representations to the Senate Subcommittee and raise troubling questions about the entities' forthrightness and transparency. *See infra* at Section III.B.3.

[115] Pacific Networks and ComNet Response, Exh. K.

[116] *Id*., Exh. K at 19-22. For purposes of citations herein to Exhibit K, pin cites associated with Exhibit K reflect the PDF pagination of the non-public business confidential filing.

[117] *Id.*, Exh. K at 26-83. {[

]} Pacific Networks and ComNet Response, Exh. K at 21.

(continued….)

]}[119] However, Pacific Networks and ComNet omitted discussion of this in responding to the *Order to Show Cause*, and represented that its indirect parent entity, CITIC Tel, "do[es] not assess or require changes in the Companies' technical or network operations."[120]

28. Pacific Networks' and ComNet's statement is further contradicted by provisions in the "CITIC Telecom IT Security Policy" that suggest the parent entity not only {[

]}

(Continued from previous page)
Material set off by double brackets {[ ]} is confidential and is redacted from the public version of this document.

[118] Pacific Networks and ComNet Response, Exh. K at 21.

[119] *Id.*, Exh. K at 21-22. {[

]} *Id.*, Exhs. A, K. *See also id.*, Exh. K at 84 {[

]}.

[120] *Id.* at 11.

[121] *Id.*, Exh. K at 21.

[122] *Id.*, Exh. K at 31.

[123] *Id.*, Exh. K at 49.

[124] *Id.*, Exh. K at 21.

[125] *Id.*, Exh. K at 21-22.

29. The "CITIC Telecom IT Security Policy" further underscores the level of control, as {[

]} Based on the record thus far, these provisions of the "CITIC Telecom IT Security Policy" appear to raise serious concerns related to Pacific Networks' and ComNet's vulnerability to the exploitation, influence, and control of the Chinese government.[128]

30. Similarly, ComNet's representations to the Senate Subcommittee and Pacific Networks' and ComNet's representations to Team Telecom show that the national security and law enforcement concerns identified are not a "theoretical potential," contrary to Pacific Networks' and ComNet's contentions.[129] The PSI Report stated that "records of Team Telecom's site visits indicate that ComNet used [CITIC Tel's] data center in Hong Kong as a backup and that ComNet's wholesale billing records 'are maintained in Hong Kong.'"[130] The PSI Report further stated that "Team Telecom's records from the 2018 site visit also note that ComNet's VoIP customer and billing records are accessible to Hong Kong personnel."[131] In contrast, information about storage and accessibility of information that ComNet provided to the Senate Subcommittee was inconsistent with the information given to Team Telecom.[132]

[126] *Id.*, Exh. K at 42 (emphasis added).

[127] *Id.*

[128] Moreover, other provisions of the "CITIC Telecom IT Security Policy," {[
]} raise national security and law enforcement concerns associated with Pacific Networks' and ComNet's ownership structure and control and the risks concerning access to their networks. {

]} *Id.*, Exh. K at 42. {[

]} *Id.*, Exh. K at 58. {

]}

[129] Pacific Networks and ComNet Response at 21 (stating that "the [*Order to Show Cause*] appears to focus on the ownership structure of the Companies and the theoretical potential that their facilities could be used to assist 'the Chinese government's involvement in computer intrusions and attacks against the United States.'").

[130] PSI Report at 96 (citing DHS00460PSI–65, at DHS00463PSI; DHS00466–71, at DHS00468PSI).

[131] *Id.* (citing DHS00466–71, at DHS00470PSI).

[132] *Id.* (stating that ComNet representatives informed the Senate Subcommittee "that its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems" and "that its parent companies do not have direct access to these records and that they would need to request access from ComNet and follow ComNet's local procedures," whereas "records of Team Telecom's site visits indicate that ComNet used [CITIC Tel's] data center in Hong Kong as a backup and that ComNet's wholesale billing records 'are maintained in Hong Kong.'") (citing Briefing with ComNet (Apr. 13, 2020); DHS00460PSI–65, at DHS00463PSI; (continued….)

31. Pacific Networks and ComNet did not address at all this information in their response to the *Order to Show Cause*, and did not otherwise indicate to the Commission that the accompanying exhibits include any relevant information about {[

]}[134] In a July 6, 2015 letter to DHS, counsel for Pacific Networks and ComNet stated, "Pacific Networks and ComNet herein confirm that, since February 13, 2014, there have been no changes to their physical and logical technical security architecture in the United States. {[

]}[135] Further, DOJ, in a June 8, 2018 letter to Pacific Networks and ComNet, stated that it received "detailed descriptions of ComNet's Domestic Communications Infrastructure within the United States and its connectivity to operations infrastructure within Hong Kong and China."[136] Thus, contrary to Pacific Networks' and ComNet's arguments, the record evidence with respect to the location of ComNet's customer and billing records in Hong Kong and potential access to such data by their parent entity or entities, combined with the consequences of Chinese intelligence and cybersecurity laws, raises significant national security and law enforcement concerns.

32. Moreover, publicly available information also indicates that Pacific Networks' and ComNet's operations are more closely associated with that of their parent entities than is apparent in their response to the *Order to Show Cause*. CITIC Tel's coverage map identifies ComNet as a "Branch."[137] CITIC Tel's website identifies one of its "Mission[s]" as "[r]ooted in Mainland China, taking Hong Kong and Macau as the base and connection, providing communications and ICT services with global coverage,"[138] and states that it "also has unique coverage in the 'Belt and Road' region."[139] CITIC Tel

(Continued from previous page)
DHS00466–71, at DHS00468PSI; Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee)).

[133] Pacific Networks and ComNet Response, Exh. K at 19-20, 24.

[134] *Id.*, Exh. K at 24.

[135] *Id.*, Exh. K at 17.

[136] *Id.*, Exh. K at 156-57. Pacific Networks and ComNet did not provide the detailed descriptions in their response to the *Order to Show Cause* and we direct Pacific Networks and ComNet to file a copy of what they provided to DOJ. *See* Appx. A.

[137] CITIC Telecom International Holdings Limited, *Corporate Profile – Coverage Map*, https://www.citictel.com/about-us/corporate-profile/ (last visited Mar. 16, 2021); CITIC Telecom International Holdings Limited, *ComNet*, https://www.citictel.com/subsidiary/%e4%bf%a1%e9%80%9a%e9%9b%bb%e8%a9%b1-comnet/ (last visited Mar. 16, 2021); *see also* CITIC Telecom International Holdings Limited, An Internet-Oriented Integrated Telecom & ICT Leader – CITIC Telecom International Company Profile at 9 (Sept. 2020) ("Global Coverage: Unique Edge in the 'Belt and Road' Regions"), https://www.citictel.com/wp-content/uploads/2020/09/CITIC-Telecom-International_Company-Profile-2020-September-eng.pdf (CITIC Telecom International Company Profile).

[138] CITIC Telecom International Holdings Limited, *Corporate Profile*, https://www.citictel.com/about-us/corporate-profile/ (last visited Mar. 16, 2021); *see also* CITIC Telecom International Holdings Limited, Interim Report 2020, https://www.citictel.com/wp-content/uploads/2020/09/e1883_20200908.pdf.

also states that it "is the InfoComm sector arm under CITIC Limited."[140] In 2017, a Vice President of CITIC Group Corporation and CITIC Limited described CITIC Tel as "'the flagship of CITIC Group in the information service sector'" and "'an important investment vehicle of the Group playing a crucial role in bringing synergies to and to full play the integrated advantages. CITIC Group is seeking to transform itself through developing 'Internet+' communication business and emerging strategic industries. The Group will also spare no effort in supporting the development of CITIC Telecom.'"[141]

33. Notwithstanding omissions of information by Pacific Networks and ComNet, the record provides ample evidence that Pacific Networks' and ComNet's parent entities are affiliated with the Chinese Communist Party. Publicly available information about Pacific Networks' and ComNet's indirect parent entities supports the concern raised both by the Executive Branch agencies and the Commission in other proceedings regarding the Chinese government's ability to influence state-owned enterprises,[142] and consequently their indirect subsidiaries, through Chinese Communist Party

(Continued from previous page)

[139] CITIC Telecom International Holdings Limited, *Message from the Chairman*, https://www.citictel.com/about-us/chairmans-statement/ (last visited Mar. 16, 2021).

[140] CITIC Telecom International Company Profile at 3. CITIC Limited, an indirect parent entity of CITIC Tel, states that "CITIC Limited's other businesses include information services," and that "CITIC Limited provides information services through two subsidiaries" which includes "CITIC Telecom International (SEHK: 1883)." CITIC Limited, *Other Businesses*, https://www.citic.com/en/our_business/other_businesses/ (last visited Mar. 16, 2021); *see also* CITIC Limited, Annual Report 2019 at 52, https://www.citic.com/uploadfile/2020/0421/20200421062822309.pdf.

[141] CITIC Telecom International Holdings Limited, *CITIC Tel Celebrates 10th Listing Anniversary* (Oct. 27, 2017), https://www.citictel.com/wp-content/uploads/2018/10/CITIC-Telecom-10th-IPO-Anniversary_E_20171026_Final.pdf; CITIC Telecom International Holdings Limited, *10th Listing Anniversary of CITIC Telecom International*, https://www.citictel.com/story/%E4%B8%AD%E4%BF%A1%E5%9C%8B%E9%9A%9B%E9%9B%BB%E8%A8%8A%E4%B8%8A%E5%B8%82%E5%8D%81%E9%80%B1%E5%B9%B4%E8%AA%8C%E6%85%B6/ (last visited Mar. 16, 2021).

[142] *See China Mobile USA Order*, 34 FCC Rcd at 3369-70, para. 18; *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15018-20, para. 23. Article 33 of the Revised Constitution of the Communist Party of China states, among other things, that "[t]he leading Party members groups or Party committees of state-owned enterprises shall play a leadership role, set the right direction, keep in mind the big picture, ensure the implementation of Party policies and principles, and discuss and decide on major issues of their enterprise in accordance with regulations." Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress, Article 33 (Oct. 24, 2017), http://www.xinhuanet.com//english/download/Constitution_of_the_Communist_Party_of_China.pdf (Revised Constitution of the Communist Party of China). Article 33 further states that "[p]rimary-level Party organizations in state-owned or collective enterprises should focus their work on the operations of their enterprise. Primary-level Party organizations shall guarantee and oversee the implementation of the principles and policies of the Party and the state within their own enterprise and shall support the board of shareholders, board of directors, board of supervisors, and manager (or factory director) in exercising their functions and powers in accordance with the law." *Id*. Article 32 states that "[p]rimary-level Party organizations play a key role for the Party in the basic units of social organization" and that their "main tasks" include "to encourage Party members and the people to consciously resist unacceptable practices and resolutely fight against all violations of Party discipline or state law." *Id*. Furthermore, Article 19 of the Company Law of the People's Republic of China (2018 Amendment) states, "[t]he Chinese Communist Party may, according to the Constitution of the Chinese Communist Party, establish its branches in companies to carry out activities of the Chinese Communist Party. The company shall provide necessary conditions to facilitate the activities of the Party." Law of China, Company Law of the People's Republic of China (2018 Amendment) at Article 19, http://lawinfochina.com/display.aspx?id=e797dd968c30e172bdfb&lib=law; *see* CITIC Group Corporation, *Corporate Governance and Risk Management*, https://www.group.citic/en/About_CITIC/Governance_Risk/ (last visited Mar. 16, 2021) ("In accordance with the Company Law and the Articles of Association, the Group further improved its governance structure in line with

(continued….)

organizations.[143] Pacific Networks and ComNet state that, with respect to "directors, officers and other senior management officials" of Pacific Networks, ComNet, and Pacific Choice International Limited, "none have any prior employment with the Chinese government or have had any affiliations with the Chinese Communist Party or the Chinese government."[144] What Pacific Networks and ComNet did not disclose, however, was any such information pertaining to their other parent entities. Based on publicly available information, the ultimate parent entity[145] has a Chinese Communist Party organization ("Group Party Committee") within its corporate leadership.[146] The corporate governance information of CITIC Group Corporation identifies the three Executive Directors as also "Party Secretary," "Deputy Party Secretary," and "Party Committee Member," respectively, of the Group Party Committee.[147] These Executive Directors of CITIC Group Corporation are also the three Executive Directors of CITIC

(Continued from previous page)
modern business operations, and the checks and balances among the Board of Directors, the Board of Supervisors and the Management, to provide the mechanisms necessary for operation efficiency.").

[143] 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 81, n.446 (2018), https://go.usa.gov/xsmGF (noting that "[t]he guiding principles" for Chinese government ownership and control are set forth in the Constitution of the People's Republic of China and the Chinese Communist Party Constitution); U.S. Trade Representative, 2020 Report to Congress on China's WTO Compliance at 8 (2021),https://go.usa.gov/xsmGM (discussing that, "a thorough examination of China's Constitution, relevant directives and pronouncements by China's leadership, legislative and regulatory measures issued by the Chinese government, China's industrial plans and the actions of the Chinese government and the Chinese Communist Party leaves no doubt that the Chinese state maintains a tight grip on virtually all economic activity."); U.S. Trade Representative, 2018 Report to Congress on China's WTO Compliance at 12 (2019), https://go.usa.gov/xsmGe (discussing that, "[t]o fulfill these [constitutional] mandates, the government and the Party direct and channel economic actors to meet the state's planning targets").

[144] Pacific Networks and ComNet Response at 11-12. The corporate governance information shows that Pacific Networks, ComNet, and Pacific Choice International Limited have identical two-person Board of Directors. *Id.*, Exhs. B and C. Pacific Networks and ComNet state that "[n]o other officers or senior officials are employed by" Pacific Networks and Pacific Choice International Limited." *Id.*, Exh. B at B-1; Exh. C at C-1. The corporate governance information identifies one individual as "Officers and Other Senior Officials" of ComNet. *Id.*, Exh. B at B-2.

[145] Pacific Networks and ComNet state that "the ultimate parent entity of the licensees is state-owned CITIC Group Corporation." *Id.* at 10; *see also* Executive Branch Letter at 2, 11-12; *Order to Show Cause*, 35 FCC Rcd at 3735, para. 4.

[146] CITIC Group Corporation, *About CITIC – The Board of Directors and Senior Management*, https://www.group.citic/en/About_CITIC/Directors_Senior/ (last visited Mar. 16, 2021) (*CITIC Group Corporation Board of Directors and Senior Management*); *see also* Michael Forsythe, *CITIC Securities, a Pillar of Finance in China, Is in Beijing's Cross Hairs* (Sept. 17, 2015), https://www.nytimes.com/2015/09/18/business/dealbook/citic-securities-investigation-china html (stating, "the CITIC Group, is one of the most prominent companies in China. Founded in 1979, the CITIC Group originally served as China's investment arm when the country was just starting to open its economy to the outside world. The sons and daughters of many of the Communist Party's senior officials in the 1980s, the so-called eight immortals, served as top executives at the conglomerate."); Yasuo Awai, *China's Citic Leading Reform of State-Owned Companies* (Nov. 29, 2014), https://asia.nikkei.com/Business/China-s-Citic-leading-reform-of-state-owned-companies (stating, "Citic is a publicly traded conglomerate that wears the face of a private company, but in reality it is also a strategic arm of the Chinese government and is close to the country's leadership."); Sophia Yan, *Chinese anti-corruption agency warns of 'major problems' in financial sector* (Feb. 5, 2016), https://money.cnn.com/2016/02/05/news/economy/china-financial-sector-corruption-risks/ (discussing "the findings by the ruling Communist Party's Central Commission for Discipline Inspection," and noting that "[m]embers of the Communist Party committee at the financial conglomerate Citic Group were accused of 'talking about business too much while seldom talking about the Party.'").

[147] *CITIC Group Corporation Board of Directors and Senior Management*.

Limited, an indirect subsidiary of CITIC Group Corporation.[148] In addition, the President and all of the five Vice Presidents (including an Executive Director) of CITIC Group Corporation are affiliated with the Group Party Committee.[149] One of the Vice Presidents is also a Non-Executive Director of CITIC Tel.[150] Further, an individual identified as a "Deputy Party Secretary" and the six individuals identified as a "Party Committee Member" of CITIC Group Corporation also constitute the senior management of CITIC Limited.[151] One such individual is affiliated with the Central Commission for Discipline Inspection of the Communist Party of China and the National Supervisory Commission.[152] Based on CITIC Group Corporation's corporate governance information, the "Chairman of the Board of Supervisors" and the two individuals identified as "Non-Employee Supervisor" on the company's Board of Supervisors appear to be affiliated with the Chinese Communist Party.[153]

34. Pacific Networks and ComNet also failed to fully respond to the directive in the *Order to Show Cause* to include "an identification of all officers, directors, and other senior management officials of entities that hold ten percent or greater ownership interest in Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."[154] Pacific Networks and ComNet submitted such information for only one entity, Pacific Choice International Limited, even though they state that "the upstream ownership structure of Pacific Networks and ComNet consists of numerous separate entities."[155] Pacific Choice International Limited is the direct parent entity of Pacific Networks.[156] Pacific Networks and ComNet assert that "the two public company entities in the ownership structure, CITIC Limited and CITIC Tel, are publicly traded companies listed on the Hong Kong Stock Exchange. As such, the identity of their respective senior management personnel is a matter of public record (and is listed on those companies' respective websites) . . . ."[157] Importantly, based on our

[148] CITIC Limited, *Board of Directors*, https://www.citic.com/en/aboutus/board_of_directors/ (last visited Mar. 16, 2021) (*CITIC Limited Board of Directors*). CITIC Limited is a publicly traded entity that is incorporated and listed in Hong Kong. *See* Pacific Networks and ComNet Response at 10, 12, Exh. A. According to Pacific Networks and ComNet, "the only two links of ownership between the ultimate parent, [CITIC Group Corporation], and [Pacific Networks and ComNet] that do not represent 100% ownership are (1) the link immediately above CITIC Limited (a public company) which aggregates 58.13% ownership, and (2) the link immediately above CITIC Tel (also a public company) which aggregates 58.12% ownership." *Id.* at 33.

[149] *CITIC Group Corporation Board of Directors and Senior Management*.

[150] *Id.*; CITIC Limited, *Senior Management*, https://www.citic.com/en/aboutus/senior_management/ (last visited Mar. 16, 2021) (*CITIC Limited Senior Management*); CITIC Telecom International Holdings Limited, Changes to the Board (Mar. 4, 2021), https://www.citictel.com/wp-content/uploads/2021/03/E_Annc_Change_of_NED_final_20210304.pdf.

[151] *CITIC Group Corporation Board of Directors and Senior Management*; *CITIC Limited Board of Directors*; *CITIC Limited Senior Management*). One of the individuals identified as a "Party Committee Member" of CITIC Group Corporation is an Executive Director of CITIC Limited. *CITIC Limited Board of Directors*.

[152] *See CITIC Limited Board of Directors* ("currently serves as leader of Discipline Inspection and Supervision Group of CITIC Group Corporation for The Central Commission for Discipline Inspection of the CPC and The National Supervisory Commission"); *CITIC Group Corporation Board of Directors and Senior Management*.

[153] *CITIC Group Corporation Board of Directors and Senior Management*.

[154] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9. As discussed in Section III.B.3, Pacific Networks' and ComNet's failure to fully respond to the *Order to Show Cause* raises troubling questions about their transparency and reliability. *See infra* at Section III.B.3.

[155] Pacific Networks and ComNet Response at 11-12.

[156] *Id.* at 10, Exh. A.

[157] *Id.* at 12.

assessment, the two directors of Pacific Networks and ComNet are Executive Directors of CITIC Tel.[158] One of the individuals is Chief Executive Officer of CITIC Tel, while the other is the Chief Financial Officer of CITIC Tel.[159] Moreover, based on publicly available information, it appears several individuals on CITIC Tel's Board of Directors hold or previously held positions in the corporate leadership of the company's parent entities, including CITIC Limited and CITIC Group Corporation.[160] CITIC Tel identifies CITIC Group Corporation and CITIC Limited as its "Major Shareholder."[161] In addition, several individuals on the Board of Directors of CITIC Group Corporation and/or CITIC Limited held positions of employment with the Chinese government, including the Ministry of Finance.[162]

35. Despite Pacific Networks' and ComNet's claims, the record evidence supports the concerns raised by the Executive Branch agencies that Pacific Networks and ComNet are subject to influence and control by the Chinese government.[163] These concerns are also supported by our understanding that Chinese law requires citizens and organizations, including state-owned entities, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world.[164] Moreover, as we observed in the *Protecting Against National Security Threats Order*, "the Chinese government is highly centralized and exercises strong control over commercial entities, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information."[165] While Pacific Networks and ComNet assert that "neither Company has been asked by the Chinese government or the Chinese Communist Party to take any action that would

---

[158] *Id.*, Exh. B.

[159] *Id.*

[160] CITIC Telecom International Holdings Limited, *About Us – Leadership*, https://www.citictel.com/about-us/leadership/ (last visited Mar. 16, 2021); CITIC Telecom International Holdings Limited, Annual Report 2019 at 71-72.

[161] CITIC Telecom International Holdings Limited, *Major Shareholder* (Feb. 17, 2021), https://www.citictel.com/about-us/major-shareholder/.

[162] *CITIC Group Corporation Board of Directors and Senior Management*; *CITIC Limited Board of Directors*.

[163] Executive Branch Letter at 2, 6-12.

[164] *See China Mobile USA Orde*r, 34 FCC Rcd at 3369, para. 17 (citing 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 (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://2017-2021.state.gov/remarks-at-press-availability/index.html ("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."); *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, 11442, paras. 46, 49; *Huawei Designation Order*, 35 FCC Rcd at 14440-42, paras. 16-17, 20.

[165] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, para. 46; *see also What China Wants* at 69-74.

'jeopardize the national security and law enforcement interests of the United States,'"[166] the record evidence suggests that their parent entities have influence over their operations and decisions, and Pacific Networks and ComNet have thus far failed to adequately respond to concerns that they are vulnerable to the exploitation, influence, and control of the Chinese government.

36. With respect to the 2017 National Intelligence Law, Pacific Networks and ComNet contend that the *Order to Show Cause* "does not explain the basis for believing that this law would apply equally to relatively small, independently-operated, U.S. domiciled companies that are not wholly-owned by the Chinese government, when the implementation of any such request would expose U.S. personnel of the Companies to considerable risk of prosecution."[167] Pacific Networks and ComNet state that "[t]he totality of ComNet's employees are subject to United States laws—either by virtue of full citizenship, their status as a green card holder or in one case an H1-B visa holder" and "[a]ny employee modifying operations at the direction of foreign influence would expose himself or herself to tremendous personal legal risk."[168] Pacific Networks and ComNet also argue that the *Order to Show Cause* "mistakenly assumes provisions of China's 2018 Company Law apply to the Companies."[169] They state that "Article 64 of the 2018 Company Law applies to a 'wholly state-owned company'" and "Pacific Networks and ComNet are not 'wholly state-owned,' but instead include significant non-CITIC ownership stakes in both CITIC Limited and CITIC Tel."[170]

37. The Commission has rejected arguments that the 2017 National Intelligence Law does not apply to U.S. subsidiaries of Chinese entities. In the *Protecting Against National Security Threats Order*, the Commission stated that "we are not persuaded to excuse these affiliates from the scope of our prohibition. One expert has noted that the nature of the Chinese system 'recognizes no limits to government power.' Irrespective of their physical location, these affiliates still remain subject to Chinese law."[171] The Commission further stated, "[t]he fact that [Huawei Technologies Company's (Huawei)] subsidiaries act outside of China does not mean that their parent company lacks influence over their operations and decisions given the strong influence that Huawei's parent companies and the Chinese government can exert over their affiliates."[172] In the 2020 *Huawei Designation Order*, the Commission "reject[ed] Huawei's claim that the National Intelligence Law does not apply to Huawei's U.S. subsidiary because . . . Chinese law does not have extraterritorial effect, and Huawei has never been asked by Chinese governmental entities to conduct espionage on behalf of the Chinese government."[173] The Commission considered "the broad sweep of Article 11 of the National Intelligence Law, which authorizes Chinese intelligence agencies to act abroad, and the Executive Branch's interpretation of the Chinese legal regime, which holds that Chinese law imposes affirmative legal responsibilities on both Chinese and foreign citizens, companies, and organizations operating in China to assist with Chinese intelligence-gathering activities."[174] Moreover, in that Order, the Commission found that "employees of

[166] Pacific Networks and ComNet Response at i.

[167] *Id.* at 26.

[168] *Id.* at 25-26.

[169] *Id.* at 22.

[170] *Id.* at 22-23 (emphasis omitted).

[171] *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11442, para. 49.

[172] *Id.* at 11446, para. 56.

[173] *Huawei Designation Order*, 35 FCC Rcd at 14441, para. 20 (citation omitted).

[174] *Id*. at 14441-42, para. 20 (citing *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs –Huawei Designation*, PS Docket No. 19-351, Order, 35 FCC Rcd 6604, 6614, para. 23 (PSHSB 2020); Letter from Douglas W. Kinkoph, Associate Administrator, Office of Telecommunications and Information Applications, National Telecommunications and Information Administration, to Ajit Pai, Chairman, (continued….)

Huawei's U.S. subsidiaries are susceptible to coercion by Huawei China, and by extension Chinese intelligence."[175] Similarly, we reject the argument that the 2017 National Intelligence Law does not apply to Pacific Networks and ComNet despite any claims that they are "relatively small, independently-operated, U.S. domiciled companies" or whose "employees are subject to United States laws."[176] In light of the Commission's statements in other proceedings, Pacific Networks and ComNet have thus far failed to adequately address concerns regarding the substantial likelihood that they would be forced to comply with Chinese government requests without the ability to challenge such requests.[177]

38. With respect to the 2018 Company Law, Pacific Networks and ComNet argue that "Pacific Networks and ComNet are not 'wholly state-owned,'" and that "Article 64 makes clear that if a company is 'invested wholly by the state,' it is subject to special provisions—provisions not applicable to the Companies that are only partially owned by the Chinese government."[178] As we noted in the *Order to Show Cause*, the Commission's records reflect that the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization, directly owns 100% of CITIC Group Corporation[179] and Pacific Networks and ComNet do not dispute that their ultimate parent entity is subject to the 2018 Company Law or that it is a wholly state-owned entity.[180] We also find unpersuasive Pacific Networks' and ComNet's argument that "[t]he Companies are thus able both in fact and in law to operate under substantially more independence than the Commission previously assumed"[181] in light of significant national security concerns identified by the Executive Branch agencies regarding Chinese intelligence and cybersecurity laws. The Executive Branch agencies state that the 2017 National Intelligence Law and 2017 Cybersecurity Law "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."[182]

39. The Executive Branch agencies further state that other provisions of Chinese law, including 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."[183] Significantly, the Executive Branch agencies state that the 2017 Cybersecurity Law "requires extensive cooperation by telecom and network operators," and the "vague

(Continued from previous page)
Federal Communications Commission, PS Docket Nos. 19-351 and 19-352; WC Docket No. 18-89, at 5 (filed June 9, 2020)).

[175] *Id*., 35 FCC Rcd at 14442, para. 21.

[176] Pacific Networks and ComNet Response at 25-26.

[177] *See China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, 11442, paras. 46, 49; *Huawei Designation Order*, 35 FCC Rcd at 14440-41, paras. 16-17; *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15018, para. 22.

[178] Pacific Networks and ComNet Response at 23 (emphasis omitted).

[179] *Order to Show Cause*, 35 FCC Rcd at 3735, 3736, 3744-45, paras. 4, 6, Appx. B. As discussed above, other publicly available information, however, indicates that CITIC Group Corporation is funded and owned by China's Ministry of Finance. *See supra* para. 5.

[180] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9. Moreover, as noted below, Pacific Networks and ComNet failed to provide "a detailed description of the current ownership and control (direct and indirect)" held by the Chinese government in the ultimate parent entity, and consequently Pacific Networks and ComNet. *See infra* Section III.B.3.

[181] Pacific Networks and ComNet Response at 23.

[182] Executive Branch Letter at 6.

[183] *Id.*

definition" of network operators "ensnares both foreign and Chinese network operators that own or manage a network or provide online services anywhere within China."[184] The Executive Branch agencies explain that the implementing regulation of the 2017 Cybersecurity Law, the 2018 "Regulation on Internet Security Supervision by Public Security Organs" (Order No. 151 of the Ministry of Public Security), "authorizes 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."[185] In addition, "[f]or remote inspections, the Ministry of Public Security would be permitted to use certain cybersecurity service agencies."[186] As discussed below, the consequences of these Chinese laws raise serious concerns with respect to Pacific Networks and ComNet.

40. Finally, we address Pacific Networks and ComNet's argument that "proceeding to revoke their [s]ection 214 authorizations" would "prevent[] them from offering services that provide a majority of the Companies' revenues,"[187] and assertion that "this is not a case where the Bureaus are seeking to deny an initial application for [s]ection 214 authority or are proposing a nominal fine or correction of a compliance failure, but instead are proposing to severely cripple a longstanding business of existing authorization holders, with adverse consequences to the Companies' customers."[188] The Commission recognizes that revocation or termination of an authorization to provide service may result in costs incurred by a service provider and that provider's customers. Where the Commission determines whether revocation is warranted, the Commission seriously considers such issues, including the impact of revocation on customers, and would revoke an authorization only for reasons consistent with the public interest. We note that national security considerations are a critical component of the Commission's public interest analysis.[189] Indeed, it is well established that one of the factors the Commission considers as part of its public interest analysis is whether the application for or retention of an authorization raises any national security, law enforcement, foreign policy, or trade policy concerns related to the applicant's or authorization holder's reportable foreign ownership.[190] In the present case concerning Pacific Networks and ComNet, we consider the national security concerns, especially those raised by the Executive Branch agencies and the PSI Report, which appear to be so serious as to warrant revocation of Pacific Networks' and ComNet's section 214 authorities.

---

[184] *Id.* at 7 (citing 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/; White Paper: Implementing China's Cybersecurity Law, Jones Day (Aug. 2017), https://www.jonesday.com/en/insights/2017/08/implementing-chinas-cybersecurity-law).

[185] *Id.* at 7-8 (citing China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems, Recorded Future Blog (Feb. 8, 2019), https://www recordedfuture.com/china-cybersecurity-measures/).

[186] *Id.* at 8.

[187] Pacific Networks and ComNet Response at 32.

[188] *Id.* at 29.

[189] *See China Mobile USA Order,* 34 FCC Rcd at 3365-66, 3376-77, 3380, paras. 8, 31-32, 38; *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11436, para. 34; *Protecting Against National Security Threats Declaratory Ruling and Second Further Notice*, 35 FCC Rcd at 7822, para. 5; *Protecting Against National Security Threats Second Report and Order*, 35 FCC Rcd at 14285, para. 2; *China Telecom Americas Order Instituting Proceedings*, 35 FCC Rcd at 15007, para. 2.

[190] *See, e.g.*, *supra* para. 4 and accompanying notes.

2. National Security and Law Enforcement Risks Associated with Pacific Networks' and ComNet's Retention of Section 214 Authorities

41. Here, we focus on the significant national security and law enforcement risks associated with Pacific Networks' and ComNet's retention of their domestic section 214 authority and international section 214 authorizations. Pacific Networks and ComNet have blanket domestic section 214 authority and each holds an international section 214 authorization.[191] Pacific Networks holds an international section 214 authorization to provide resale service on all U.S. international routes, except U.S.-China and U.S.-Hong Kong.[192] On the U.S.-China and U.S.-Hong Kong routes, Pacific Networks is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services).[193] ComNet holds an international section 214 authorization to provide facilities-based and resale service between the United States and all permissible foreign points, except China and Hong Kong.[194] On the U.S.-China and U.S.-Hong Kong routes, ComNet is authorized to provide switched services solely through the resale of unaffiliated U.S. facilities-based carriers' international switched services (either directly or indirectly through the resale of another U.S. resale carrier's international switched services).[195] Pacific Networks and ComNet state that Pacific Networks provides MPLS VPN services, which they "consider [] to be within the scope of the services Pacific Networks is authorized to provide under its domestic and international [s]ection 214 authorization granted by the Commission."[196] Pacific Networks and ComNet state that ComNet's Wholesale IDD Service and Retail Calling Card Service are services that "ComNet is authorized to provide under its international [s]ection 214 authorization granted by the Commission."[197] Importantly, while Pacific Networks and

[191] *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740, Appx. A, para. 1.

[192] *Id.*, 35 FCC Rcd at 3742-43, Appx. A, paras. 5-6; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384.

[193] *Order to Show Cause*, 35 FCC Rcd at 3742-43, Appx. A, paras. 5-6; April 23, 2009 Grant Public Notice, 24 FCC Rcd at 6384.

[194] *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740-42, Appx. A, paras. 2-4; May 7, 2009 Grant Public Notice, 24 FCC Rcd at 5379; *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-214-19990927-00607, Public Notice, 24 FCC Rcd 5779, 5784 (IB 2009) (May 21, 2009 Grant Public Notice).

[195] *Order to Show Cause*, 35 FCC Rcd at 3734, para. 2; *id.* at 3740-42, Appx. A, paras. 2-4; May 21, 2009 Grant Public Notice, 24 FCC Rcd at 5784.

[196] Pacific Networks and ComNet Response at 12-13. Pacific Networks and ComNet state that Pacific Networks' "MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States and internationally." *Id.* at 12. According to Pacific Networks and ComNet, "Pacific Networks does not provide the international circuits required for international MPLS VPN," as those facilities "are purchased from unaffiliated international carriers by Pacific Networks' wholesale customer . . . and then interconnected with Pacific Networks' VPN platform in the United States." *Id.* Pacific Networks and ComNet state that "Pacific Networks purchases from U.S. telecommunications carriers high-speed data connections to customer locations to facilitate provision of the service." *Id.* at 12-13. Pacific Networks and ComNet state that they "reserve and in no way waive the argument that the MPLS VPN services provided by Pacific Networks may not, in fact, require a [s]ection 214 authorization." *Id.* at 13, n.33.

[197] *Id.* at 13-14. Pacific Networks and ComNet state that ComNet provides Wholesale International Direct Dial (IDD) service, "handling international voice traffic and facilitating least cost routing for carriers located in the U.S. and in foreign locations. ComNet can provide this service through traditional TDM or through IP technology via SIP." *Id.* at 13. Pacific Networks and ComNet also state that ComNet "operates a retail calling card service in the United States, issuing either printed or digital phone cards with a set of 10-digit PIN numbers for international and domestic voice calls accessed via local or toll free numbers." *Id.* at 14.

ComNet identify that they offer these services pursuant to section 214 authority,[198] Pacific Networks' and ComNet's authorizations provide them with the opportunity, for example, to extend or upgrade their existing networks and provide other telecommunications services subject to the terms of their current authorizations without seeking further section 214 approval from the Commission.[199]

42. The Executive Branch agencies assert that "[t]he national security environment has changed significantly since 2009, when the Commission last granted the Companies' [s]ection 214 authorizations to provide international common carrier services."[200] The Executive Branch agencies state that "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."[201] The Executive Branch agencies add that "[t]hese 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."[202] The Executive Branch agencies cite to the 2019 Office of the Director of National Intelligence worldwide 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."[203] The Executive Branch agencies state that the U.S. intelligence community and other agencies have raised repeated warnings concerning the national security threats presented by the Chinese government's activities involving espionage.[204] According to the

[198] Pacific Networks and ComNet state that ComNet's Wholesale Short Message Service and Website/WeChat Service are services that do "not require [s]ection 214 authorization." *Id.* at 14-15. Pacific Networks and ComNet state that ComNet "provides a cloud-based Voice over Internet Protocol ('VoIP') service" and that "[t]he Commission has not required providers to obtain [s]ection 214 authorizations for the provision of interconnected VoIP." *Id.* at 14.

[199] 47 CFR §§ 63.22(a), (b); 63.23; 63.18; *see Streamlining Order*, 11 FCC Rcd at 12885-93, 12894-96, paras. 2-19, 21-26 (adopting rules, among other things, to issue global international section 214 authorizations to facilities-based carriers for the provision of international services pursuant to which "authority will be given to use half-circuits on all U.S. common carrier and non-common carrier facilities previously and subsequently authorized by the Commission and on any necessary foreign connecting facilities," and "to allow resellers to provide international resale of switched or private line services via any authorized carrier, except U.S. facilities-based affiliates that are regulated as dominant on routes the carrier seeks to serve."); *1998 Biennial Regulatory Review—Review of International Common Carrier Regulations*, Report and Order, 14 FCC Rcd 4909, 4910, 4911, 4933-34, paras. 2, 6, 57-61 (1999).

[200] Executive Branch Letter at 2.

[201] *Id.* at 9.

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

[203] *Id.* at 3 (citing 2019 ODNI Threat Assessment). Moreover, the Executive Branch agencies state that "[t]he pervasiveness of this cyber-enabled espionage is reflected in the 2019 ODNI Threat Assessment, which warns not only of the [Chinese] 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.'" *Id.* at 5 (citing 2019 ODNI Threat Assessment at 5) (emphasis added).

[204] *Id.* at 3-4 (citing, for example, 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); 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://go.usa.gov/xss7w; *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, 2018) (statement of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland

(continued….)

Executive Branch agencies, "[i]n its November 2018 Update to its Section 301 findings, the [Office of the U.S. Trade Representative] stated that incidents of Chinese cyber thefts were rapidly accelerating."[205] The Executive Branch agencies assert that "[t]hese repeated warnings" are "supported by a number of public law enforcement actions against Chinese actors."[206]

43. The Executive Branch agencies state that "[m]uch like the national security environment, [Pacific Networks and ComNet] are not the same providers today that they were when they executed the Letter of Assurance."[207] The Executive Branch agencies assert that "[s]imilar to [China Mobile USA's] anticipated customers, [Pacific Networks' and ComNet's] customers also include fixed and mobile network operators, wholesale carriers, and calling card customers," and "[t]he Executive Branch judged that the Chinese government could exploit [China Mobile USA's] interconnections and access to U.S. companies and data."[208] The Executive Branch agencies state that "[t]he 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."[209]

44. The Executive Branch agencies state that Pacific Networks and ComNet, "as international [s]ection 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."[210] The Executive Branch agencies assert that "[s]uch connections and access can provide a strategic capability to target, collect, alter, block, and re-route network traffic."[211] The Executive Branch agencies further state that "[t]his 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."[212] The Executive Branch agencies assert that "[t]he [Chinese] government could use [Pacific Networks' and ComNet'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."[213] The Executive Branch agencies state that "the [Chinese] government,

(Continued from previous page)
Security), https://go.usa.gov/xss7f; 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), https://go.usa.gov/xss7H; 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://go.usa.gov/xss7A; 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://go.usa.gov/xss7s (USTR Update Concerning China's Acts, Policies and Practices).

[205] *Id.* at 4 (citing USTR Update Concerning China's Acts, Policies and Practices at 10-22).

[206] *Id*. The Executive Branch agencies state that "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." *Id*. at 5.

[207] *Id*. at 8.

[208] *Id.* (citing Pacific Networks and ComNet Response at 13-15; Executive Branch Recommendation to Deny at 15).

[209] *Id.*

[210] *Id.* at 10.

[211] *Id.*

[212] *Id*.

[213] *Id.*

through [Pacific Networks and ComNet], would have a greater ability to monitor, degrade, and disrupt U.S. government communications."[214] The Executive Branch agencies also state that "due to least-cost routing, the communications of U.S. government agencies to any international destinations may conceivably pass through [Pacific Networks' and ComNet's] network during transit, even if the agencies are not actual customers of the Companies."[215] The Executive Branch agencies argue that "[s]o long as [Pacific Networks and ComNet] control their network, the traffic transmitting this network remains subject to exploitation, influence, and control by the Chinese government."[216]

45. In addition, Pacific Networks' and ComNet's U.S.-based Points of Presence are highly relevant to concerns about security related to Chinese government-affiliated entities.[217] As researchers have noted, because little traffic goes through China's mainland nodes and there is much more traffic through the significantly larger number of access points by carriers with operations in the U.S., there is greater opportunity for malicious behavior in the United States.[218] Pacific Networks and ComNet, like any similarly situated service provider, are part of this security concern. In particular, Pacific Networks' MPLS VPN service involves the use of Points of Presence to peer with other providers using Border Gateway Protocol (BGP) routers.[219] As noted in Appendix A, we inquire about the locations where Pacific Networks provides this BGP connectivity. Likewise, ComNet provides VoIP service, which requires IP connectivity achieved by BGP. We also inquire in Appendix A about the structure of this VoIP service. Among the potential concerns, like other similarly situated providers, ComNet may be able to use BGP routers to forward to China interconnected VoIP traffic,[220] maliciously or accidentally, without the knowledge or authorization of the customer, and for purposes that may include espionage or threats to U.S. national security.[221] Ultimately, Pacific Networks' and ComNet's Points of Presence in the United States are concerning because of the role of their parent entities in their management and oversight as described above, and Pacific Networks' and ComNet's resulting vulnerability to exploitation, influence, and control by the Chinese government through their parent entities. This vulnerability presents opportunities for the Chinese government to conduct activities that would ultimately pose

[214] *Id.*

[215] *Id.*

[216] *Id.* at 11.

[217] In Exhibit D, Pacific Networks and ComNet identify a "New York PoP address" and a "Los Angeles PoP address" in association with Pacific Networks. Pacific Networks and ComNet Response, Exh. D at D-1. Pacific Networks and ComNet also identify an "LA-IDC" in Los Angeles associated with ComNet. *Id.*, Exh. D at D-5.

[218] *See* Chris C. Demchak & Yuvall Shavit, *China's Maxim: Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking*, Military Cyber Affairs vol. 3 issue 1 (2018).

[219] We note that the offering of IP Transit services in the form of using the BGP is a prime candidate for security exploitation. For many years, BGP hijacking has been used maliciously to redirect Internet traffic towards a specific provider that in turn would have the ability to examine that traffic through Deep Packet Inspection (which examines the contents of a packet) or store traffic for later examination. By offering BGP-based IP transit service, the hijacking of routes and examination of data can be accomplished in ways that are not apparent to clients or peering providers. *See* Cloudflare, *What is BGP Hijacking?*, https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/ (last visited Mar. 15, 2021).

[220] *See* Center for Applied Internet Data Analysis (CAIDA), *HIJACKS: Detecting and Characterizing Internet Traffic Interception based on BGP Hijacking*, https://www.caida.org/funding/hijacks/hijacks_proposal.xml (last visited Mar. 15, 2021).

[221] *See* Andra Tatu et al., A First Look at the IP eXchange Ecosystem, ACM SIGCOMM Computer Communication Review (Oct. 2020), https://arxiv.org/pdf/2007.13809.pdf; *see* Catalin Cimpanu, *China has been "hijacking the vital internet backbone of western countries"* (Oct. 26, 2018), https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/.

significant threats to U.S. national security and law enforcement interests.

46. The national security and law enforcement risks associated with Pacific Networks' and ComNet's retention of their section 214 authorities are based, in part, on concerns that service providers such as Pacific Networks and ComNet, by virtue of controlling the systems or infrastructure, are in a unique position to use this access to exploit their customers' vulnerabilities on the network and, unlike other service providers with similar systems or infrastructure, may be directed to do so. A service provider is authorized pursuant to its contract with the customer to provide specific service(s) and, for example, can and will monitor traffic (e.g., metadata from packets) and manipulate services supported by its infrastructure to ensure quality.[222] The service provider has control of the systems or infrastructure, including the applications and servers, depending on the service. Moreover, even if the service provider does not control applications or servers, it can analyze application content or metadata derived from packets transiting its network or infrastructure that it manages.[223] The service provider also has some level of control over the security of the systems and infrastructure (e.g., access control) and has the ability to obtain access to the systems or infrastructure to examine or reroute data and metadata. Once acquired, the data can be examined and possibly manipulated to counter customer data security measures that may be present.[224] This risk exists regardless of the type of telecommunications service and has been noted by both industry groups and independent researchers.[225] To the extent the provider does not engage in further access, this is because it is not authorized to so, and not because it is technically unable to do so.[226] Importantly, from the customer's perspective, it may be impossible to distinguish between the monitoring and manipulation of traffic that is authorized (i.e., within the scope of the contract) and that which is unauthorized (i.e., outside the scope of the contract).[227]

47. Communication network vendors and providers, including Pacific Networks and ComNet and many others, offer a variety of products and services that facilitate the exchange of voice, data, and other information between two or more endpoints (e.g., server, laptop, smart phone) in a network. In

---

[222] Allowing unauthorized access to Customer Proprietary Network Information (CPNI) is a violation of section 222 of the Act as well as Commission rules implementing section 222. *See* 47 U.S.C. § 222; 47 CFR §§ 64.2001-2011.

[223] *See* Kathleen Moriarty, *They Are Looking at What? Service Provider Monitoring* (June 14, 2018), https://blog.apnic net/2018/06/14/they-are-looking-at-what-service-provider-monitoring.

[224] *See* Karen Scarfone & Peter Mell, National Institute of Standards and Technology (NIST), *Guide to Intrusion Detection and Protection Systems,* NIST Special Publication 800-94, Sec. 4 – Network-Based IDPS (2007) https://csrc nist.gov/publications/detail/sp/800-94/final (discussing type of intrusions and best practices to prevent their success) (NIST Guide to Intrusion Detection and Prevention Systems).

[225] *See, e.g.,* GSMA, *Mobile Telecommunications Security Threat Landscape* (Jan. 2019), https://www.gsma.com/security/wp-content/uploads/2019/03/GSMA-Security-Threat-Landscape-31.1.19.pdf; Upturn, *What ISPs Can See: Clarifying the technical landscape of the broadband privacy debate* (Mar. 2016), https://www.upturn.org/reports/2016/what-isps-can-see/.

[226] *See* Dan Patterson, *Deep Packet Inspection: The Smart Person's Guide* (Mar. 9, 2017), https://www.techrepublic.com/article/deep-packet-inspection-the-smart-persons-guide/.

[227] *See* Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, National Institute of Standards and Technology (NIST), Zero Trust Architecture, NIST Special Publication 800-207, at Sec. 5 – Threats Associated with Zero Trust Architecture (2020), https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf (discussing denial of service as well as stolen credentials); Ramaswamy Chandramouli & Doron Pinhas, National Institute of Standards and Technology (NIST), Security Guidelines for Storage Infrastructure, NIST Special Publication 800-209, at Sec. 3.3 – Attack Surfaces (2020), https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems pursuant to the Federal Information Security Modernization Act of 2014. NIST, 2019 NIST/ITL Cybersecurity Program Annual Report, NIST Special Publication 800-211 (2020), https://nvlpubs nist.gov/nistpubs/SpecialPublications/NIST.SP.800-211.pdf.

nearly every case, cybersecurity protection of the voice, data, and/or signaling is not an inherent part of the service. The fundamental responsibilities of a network/telecommunications service provider consist of providing its customers the connectivity or service contracted, such as access to voice and data, interconnection, and transmission. The risks of cybersecurity attacks are greatest when bad actors have access to the routers, switches, servers (the devices) that store or forward traffic through their network.[228] Even if the traffic is end-to-end encrypted, the service provider can collect information on the traffic. Depending on the application, the service provider can perform traffic analysis to the point that the service provider may be able to decrypt and generate transcripts of strongly end-to-end encrypted voice calls, including calls transmitted using IP, that traverse its network.[229]

48. Pacific Networks and ComNet state that ComNet provides a cloud-based VoIP service by which "customers can make both national and international calls through ComNet's VoIP platform using certified IP phones."[230] The record does not fully explain the IP service offering or whether this is an interconnected VoIP service offering as defined by the Commission's rules and does not show security measures that Pacific Networks and ComNet may employ with this service.[231] As a general matter, security issues associated with interconnected VoIP include lack of end-to-end confidentiality and integrity.[232] With respect to confidentiality, many voice providers claim to support end-to-end security. However, voice calls between two end-point devices are often realized as a collection of different call segments, where the service provider performs decryption and re-encryption of the voice traffic. Hence,

[228] *See* NIST Guide to Intrusion Detection and Prevention Systems at Sec. 4 – Network-Based IDPS (discussing type of intrusions and best practices to prevent their success).

[229] *See* Andrew M. White et al., Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on fon-iks (May 2011), http://www.ieee-security.org/TC/SP2011/sp11-toc.html (Proceedings of the 2011 IEEE Symposium on Security and Privacy); Charles V. Wright et al., *Spot me if you can: Uncovering spoken phrases in encrypted VoIP conversation* (May 2008), https://ieeexplore.ieee.org/document/4531143 (Proceedings of the 2008 IEEE Symposium on Security and Privacy).

[230] Pacific Networks and ComNet Response at 14. Pacific Networks and ComNet state that "[t]he Commission has not required providers to obtain [s]ection 214 authorizations for the provision of interconnected VoIP." *Id.* Pacific Networks and ComNet also state that ComNet offers Website/WeChat Service, described as "website development and hosting services," where it "is responsible for the website layout and framework design, content processing and maintenance support." *Id* at 15. Pacific Networks and ComNet note that "[t]he websites are hosted in ComNet's datacenter or other hosting service platform provided by the customer." *Id.* Pacific Networks and ComNet state that "[t]hese services do not require [s]ection 214 authorization." *Id.* The record does not show security mechanisms or protocols, such as for transmission or storage of media, that may be provided by Pacific Networks and ComNet. We note there have been reports that China has been intercepting WeChat texts from the United States and other countries. Emily Feng, *China Intercepts WeChat Texts From U.S. And Abroad, Researchers Say* (Aug. 29, 2019), https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says.

[231] We direct Pacific Networks and ComNet to fully explain the IP service offering or whether this is an interconnected VoIP service offering as defined by the Commission's rules and any security measures concerning this service. *See* Appx. A.

[232] Security issues associated with interconnected VoIP also include its proclivity for being used to originate illegal robocalls whose originating number is masqueraded or spoofed as a fake number. The STIR/SHAKEN framework, an industry-standard caller ID authentication technology, is a set of technical standards and protocols that allow for the authentication and verification of caller ID information for calls carried over Internet Protocol (IP) networks. *See* FCC, *Combating Spoofed Robocalls with Caller ID Authentication*, https://www fcc.gov/call-authentication (last visited Mar. 10, 2021). STIR/SHAKEN are acronyms for the Secure Telephone Identity Revisited and Signature-based Handling of Asserted Information Using toKENs standards. *Id.* The Commission has mandated that all voice service providers implement the STIR/SHAKEN caller ID authentication framework in the Internet Protocol (IP) portions of their networks by June 30, 2021. *See Call Authentication Trust Anchor*; *Implementation of TRACED Act Section 6(a) — Knowledge of Customers by Entities with Access to Numbering Resources*, Report and Order and Further Notice of Proposed Rulemaking, 35 FCC Rcd 3241 (2020).

while the voice portion of the call is protected between two network devices, its decryption within the network allows bad actors to see the information in the clear and gain knowledge of what is being said between two individuals. Thus, voice traffic is never truly encrypted end-to-end because of its decryption within the provider's network.

49. The Chinese government's potential access to Pacific Networks' MPLS VPN service offered pursuant to its section 214 authority raises national security or law enforcement concerns.[233] Pacific Networks and ComNet state that Pacific Networks provides "multi-protocol label switching virtual private networks ('MPLS VPN') services,"[234] and they identify {[ ]} to whom Pacific Networks provides "international services."[235] With respect to MPLS VPN, this is a service based on a suite of protocols that encapsulates packets with an MPLS defined header and then forwards the traffic through a virtual private network.[236] Internet Protocol Security (IPsec) may be used to provide end-to-end confidentiality through the VPN, though it is not inherent in MPLS. In addition, the "end" of an MPLS service is the ingress edge of a provider, which means confidentiality is only offered within the provider network. As a result, unencrypted IP packets sent by clients to the MPLS edge, even if the service provider offers an encrypted VPN offering, can be examined, stored, and altered by the provider.[237]

50. The PSI Report stated that ComNet "leverages [CITIC Tel's NOC], located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions. 'All system alarms and network management data are sent to the NOC . . . .' Further, [CITIC Tel's] NOC maintains records of all alarms and access logs generated by ComNet's systems."[238] Generally, a NOC oversees the operation of the network through management tools that monitor the network by constantly gathering information (e.g., packet loss) and storing it in the NOC, and at times (re)configures various parts of the infrastructure, which can be comprised of forwarding devices (e.g., routers, hubs, switches) as well servers or data centers used to store vast amounts of information.[239] The recent discovery of the compromised network management software from SolarWinds shows the interest by bad actors in accessing the information that can be gathered by a NOC.[240] Metadata gathered by this Hong Kong-based NOC, as well as the ability of the NOC and its operator to re-route data traffic to international locations, adds to the security risk for U.S. clients. In addition, regardless of the location of the NOC that serves ComNet, these disclosures in the PSI Report are troubling given the national security and law enforcement risks associated with Pacific

[233] Pacific Networks and ComNet Response at 12-13.

[234] *Id*. at 12.

[235] *Id.*, Exh. E. Pacific Networks and ComNet describe "[i]nternational services" as "virtual private network services provided to customers with at least one end customer site in the United States and other end customer site(s) outside the United States." *Id.*

[236] *See* Internet Engineering Task Force (IETF), Request For Comments: 3031, Category: Standards Track, Multiprotocol Label Switching Architecture (Jan. 2001), https://tools.ietf.org/html/rfc3031.

[237] For further discussion of the limitations of MPLS in the context of security, *see Security Issues Not Addressed by the MPLS Architecture*, http://etutorials.org/Networking/MPLS+VPN+security/Part+II+Advanced+MPLS+VPN+Security+Issues/Chapter+3.+MPLS+Security+Analysis/Security+Issues+Not+Addressed+by+the+MPLS+Architecture/ (last visited Mar. 4, 2020).

[238] PSI Report at 96 (citing Briefing with ComNet (Apr. 13, 2020); DHS00460PSI–65, at DHS00462PSI).

[239] *See* Cisco, *Network Management System: Best Practices White Paper* (Aug. 10, 2018), https://www.cisco.com/c/en/us/support/docs/availability/high-availability/15114-NMS-bestpractice html.

[240] *See* FireEye, *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor* (Dec. 13, 2020), https://www fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor html.

Networks' and ComNet's parent entities discussed above.[241]

51. In addition, Pacific Networks' and ComNet's service offerings provide them with access to personally identifiable information (PII) and CPNI concerning their customers, and this access presents risks related to the protection of sensitive customer information and the effectiveness of U.S. law enforcement efforts. As noted, Pacific Networks and ComNet state that Pacific Networks provides MPLS VPN services pursuant to its domestic and international section 214 authority[242] and that ComNet provides Whole International Direct Dial (IDD) Service and Retail Calling Card Service pursuant to its international section 214 authorization.[243] We note that Pacific Networks and ComNet are likely to have access to significant amounts of customer PII, including billing information such as name and address, payment details such as credit card numbers, and other data.[244] Pacific Networks and ComNet are also likely to have access to a customer's usage information, including date and time of incoming and outgoing voice and data communications, the identity of the sending or receiving party, details on data usage, and more.[245] Such usage information could be combined with a customer's PII to provide

[241] We note that these concerns also pertain to Pacific Networks and ComNet's data centers. Pacific Networks and ComNet refer to ComNet's "datacenter in One Wilshire Building, Los Angeles." Pacific Networks and ComNet Response at 16; *see also id.* at 8 (referring to "the Companies' Los Angeles data center"). A provider, including Pacific Networks and ComNet, can also offer data hosting and processing. The data are hosted on servers at colocation sites or data farms. The service provider may simply provide a platform such as hosting, cloud, or an ecommerce backend, or it may provide application services such as messaging and voice. The service provider may be contracted to store, monitor, manipulate, mirror, and manage the data and the processing. At the application layer, the threats include loss of data, theft of data, and theft of service.

[242] *Id.* at 12-13. Pacific Networks and ComNet state that Pacific Networks' "MPLS VPN service provides data communications that enable its customers to operate business applications among various customer sites both within the United States and internationally." *Id.* at 12. According to Pacific Networks and ComNet, "Pacific Networks does not provide the international circuits required for international MPLS VPN," as those facilities "are purchased from unaffiliated international carriers by Pacific Networks' wholesale customer . . . and then interconnected with Pacific Networks' VPN platform in the United States." *Id.* Pacific Networks and ComNet state that "Pacific Networks purchases from U.S. telecommunications carriers high-speed data connections to customer locations to facilitate provision of the service." *Id.* at 12-13.

[243] *Id.* at 13-14. Pacific Networks and ComNet state that ComNet provides Wholesale International Direct Dial (IDD) service, "handling international voice traffic and facilitating least cost routing for carriers located in the U.S. and in foreign locations. ComNet can provide this service through traditional TDM or through IP technology via SIP." *Id.* at 13.

[244] *See TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13331, para. 17 (2014) (stating that "[i]n general, PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context"); 47 CFR § 64.2002(m).

[245] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Declaratory Ruling, 28 FCC Rcd 9609, 9611, para. 9 (2013) (stating that CPNI "includes information about a customer's use of the service that is made available to the carrier by virtue of the carrier-customer relationship. As the Commission has explained, '[p]ractically speaking, CPNI includes information such as the phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting'" (quoting *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, 6931, para. 4 (2007))). Congress defined CPNI to include "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship," demonstrating the intent to confer a higher level of protection to this type of information. 47 U.S.C. § 222(h)(1). While CPNI and PII are separately defined, they are not mutually

(continued….)

significant details to Pacific Networks and ComNet and their parent entities, potentially providing opportunities for Chinese government-sponsored actors to engage in information collection activities or espionage of U.S. targets,[246] or for any other activities that are contrary to the protection of U.S. customer records and U.S. interests. Further, Pacific Networks and ComNet must be capable of complying with legal requests for information issued by the U.S. government, as required by the Communications Assistance for Law Enforcement Act (CALEA).[247] Pacific Networks and ComNet would therefore have knowledge of U.S. government requests concerning electronic surveillance for which their assistance is requested as well as knowledge of any government requests for access to customer records. Pacific Networks' and ComNet's vulnerability to the exploitation, influence, and control of the Chinese government raises questions as to whether they can be trusted to cooperate with the U.S. government and hold in confidence the fact that such legal requests concerning surveillance have been received, the content therein, and the records produced in response to the requests. To the extent that Pacific Networks and ComNet, or any similarly situated provider, is not a trusted provider, this lack of trust could seriously undermine the protection of U.S. customer records and the efforts of U.S. law enforcement agencies. Based on the foregoing, there appear to be significant national security and law enforcement risks associated with Pacific Networks' and ComNet's capabilities pursuant to their section 214 authority, which raise significant concerns as to whether retention of their section 214 authority remains in the public interest.

3. Pacific Networks' and ComNet's Representations to the FCC and Other U.S. Government Agencies

52. Pacific Networks' and ComNet's representations to the Commission and to other U.S. government agencies raise significant concerns regarding whether Pacific Networks and ComNet should retain their domestic section 214 authority and international section 214 authorizations. First, we find that Pacific Networks and ComNet failed to fully respond to the Bureaus' questions in the *Order to Show Cause* and omitted crucial information in this proceeding that was disclosed to the Senate Subcommittee and published in the PSI Report. Second, Pacific Networks and ComNet failed to comply with the Commission's rules requiring notification of a *pro forma* transfer of control. Based on the record evidence, we question Pacific Networks' and ComNet's transparency and reliability and have reservations regarding their ability to fully to cooperate with the Executive Branch agencies and the U.S. government generally. Pacific Networks' and ComNet's truthfulness with the Commission and the U.S. government, and their ability to comply with the Commission's rules, are essential qualities for establishing that the public interest, convenience, and necessity is served by Pacific Networks' and ComNet's retention of their section 214 authorities.

(Continued from previous page)
exclusive (i.e., a carrier is privy to information due to its relationship with the customer (CPNI) that could also be used to identify the individual (PII)).

[246] Executive Branch Letter at 8, 10. In addition to Pacific Networks' and ComNet's immediate access to this information, the record indicates that their indirect parent CITIC Tel also has access to this information maintained in Hong Kong. PSI Report at 96 (stating that "records of Team Telecom's site visits indicate that ComNet used [CITIC Tel's] data center in Hong Kong as a backup and that ComNet's wholesale billing records 'are maintained in Hong Kong'") (citing DHS00460PSI–65, at DHS00463PSI; DHS00466–71, at DHS00468PSI).

[247] Pacific Networks and ComNet Response at 26. *See also* Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1002(a) (stating, "a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of," among other things, "expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government[.]").

53. *Failure to Fully Respond to Order to Show Cause Questions.* Based on the PSI Report, it appears that ComNet did not provide the Commission with the same information that it provided to the Senate Subcommittee and was disclosed in the PSI Report[248] concerning the extent of the involvement and control of its indirect parent corporation, CITIC Tel,[249] as required by the *Order to Show Cause*.[250] Pacific Networks and ComNet failed to identify the Chinese government entity and the percentage of ownership interest that the entity holds in CITIC Group Corporation, as required by the *Order to Show Cause.*[251] Finally, Pacific Networks and ComNet failed to fully disclose all officers, directors, and other senior management of entities that hold ten percent or greater ownership interest in Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government, as required by the *Order to Show Cause*.[252]

54. First, based on the information in the PSI Report, Pacific Networks' and ComNet's indirect parent company, CITIC Tel, appears to have greater involvement and control over the management and operations of ComNet than was described by Pacific Networks and ComNet in their response to the *Order to Show Cause*. The *Order to Show Cause* required Pacific Networks and ComNet to provide a detailed description of Pacific Networks' and ComNet's ownership and control (direct and indirect) and directed Pacific Networks and ComNet to provide "a detailed description of their corporate governance."[253] In their response, Pacific Networks and ComNet make various statements to imply that Pacific Networks and ComNet are independent from entities upstream in their ownership structure and that such entities have limited involvement in Pacific Networks' and ComNet's day-to-day management. For example, Pacific Network and ComNet state that "[i]n terms of day-to-day management, [Pacific Networks and ComNet] conduct their operations independently" and "[e]ntities upstream of [Pacific Choice International Limited] are not involved in the daily business or operations of Pacific Networks or ComNet."[254] Pacific Networks and ComNet add that "[t]he financial positions of Pacific Networks and ComNet are routinely reviewed by CITIC Tel, but they do not assess or require changes in the Companies' technical or network operations."[255] ComNet representatives similarly informed the Senate Subcommittee that its daily operations are managed by its local management team in California.[256]

55. ComNet, however, provided critical information to the Senate Subcommittee concerning the level of CITIC Tel's control over ComNet that appears to undermine its representations to the Commission. For example, ComNet informed the Senate Subcommittee that "[CITIC Tel] . . . guides ComNet on its information security policies" and "ComNet maintains a company-specific policy, but that policy was drafted based on [CITIC Tel's] guidance."[257] ComNet added that "ComNet leverages [CITIC Tel's NOC], located in Hong Kong, for 'first tier monitoring' against cyber incidents or disruptions.'"[258]

[248] PSI Report at 95-97; Pacific Networks and ComNet Response.

[249] Pacific Networks and ComNet Response, Declaration of Li Ying (Linda) Peng (identifying CITIC Tel as a "parent corporation").

[250] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[251] Pacific Networks and ComNet Response at Exh. A; *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[252] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[253] *Id*.

[254] Pacific Networks and ComNet Response at 11.

[255] *Id*.

[256] PSI Report at 95 (Briefing with ComNet (Apr. 13, 2020)).

[257] *Id*. at 95-96 (citing Briefing with ComNet (Apr. 13, 2020)).

[258] *Id*. at 96 (citing Briefing with ComNet (Apr. 13, 2020).

ComNet has also stated that "'[a]ll system alarms and network management data are sent to the NOC'" and "[CITIC Tel's] NOC maintains records of all alarms and access logs generated by ComNet's systems."[259] ComNet's failure to provide this information to the Commission concerning the level of CITIC Tel's control suggests that the information in its filing with the Commission may be incomplete or misleading. While Pacific Networks and ComNet included unredacted copies of their correspondences with Team Telecom that appear to allude to certain of the information that ComNet provided to the Senate Subcommittee,[260] Pacific Networks and ComNet failed to explain or disclose any of this information in their response to the Bureaus' questions, and made representations in their response that appear to contradict the information in those correspondences and in the PSI Report.

56. Even more troubling is that ComNet may not have been transparent with the Senate Subcommittee and the Commission concerning the location of U.S. customer records and the level of CITIC Tel's control and involvement. ComNet representatives informed the Senate Subcommittee that "its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems."[261] ComNet also informed the Senate Subcommittee that "its parent companies do not have direct access to these records and that they would need to request access from ComNet and follow ComNet's local procedures."[262] As disclosed in the PSI Report, however, records of Team Telecom's site visits clearly contradict what ComNet disclosed to the Senate Subcommittee. According to records of Team Telecom's site visits, "ComNet used [CITIC Tel's] data center in Hong Kong as a backup and . . . ComNet's wholesale billing records 'are maintained in Hong Kong.'"[263] The PSI Report added that "Team Telecom's records from the 2018 site visit also note that ComNet's VoIP customer and billing records are accessible to Hong Kong personnel."[264] Pacific Networks' and ComNet's public filing with the Commission did not describe the scope and level of CITIC Tel's control, and while Pacific Networks and ComNet did provide copies of their correspondences with Team Telecom, which the Senate Subcommittee may also have had access to, Pacific Networks' and ComNet's statements to the Commission concerning the level of CITIC Tel's control suggest that none of their indirect parent entities are involved in these matters.[265] We expect Commission regulatees to be fully transparent and forthright in their dealings with and responses to Commission inquiries without Commission staff having to examine every document to understand the level of control of Pacific Networks' and ComNet's parent entities when that question was asked by the Bureaus in the *Order to Show Cause*. Further, as noted above, concerning the level of control, we found provisions in the "CITIC Telecom IT Security Policy" that suggest the parent entity not only {[

]}[266]

57. Second, the *Order to Show Cause* requested "a detailed description of the current ownership and control (direct and indirect) of the companies and the place of organization of each entity in the ownership structure,"[267] and Pacific Networks and ComNet failed to identify the government entity

[259] *Id*. (citing to Team Telecom's records from a site visit, DHS00460PSI–65, at DHS00462PSI).

[260] Pacific Networks and ComNet Response, Exh. K.

[261] PSI Report at 96 (citing Briefing with ComNet (Apr. 13, 2020)).

[262] *Id.* (citing Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee)).

[263] *Id*. (citing DHS00460PSI–65, at DHS00463PSI; DHS00466–71, at DHS00468PSI).

[264] *Id*. (citing DHS00466–71, at DHS00470PSI).

[265] Pacific Networks and ComNet Response at 25.

[266] *Id*., Exh. K at 21; *see supra* para. 28.

[267] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

that owns CITIC Group Corporation as well as that entity's ownership interest in CITIC Group Corporation. For example, Pacific Networks and ComNet state that "the ultimate parent entity of the licensees is state-owned CITIC Group Corporation."[268] However, the ownership chart in Exhibit A does not include the Chinese government (neither generally nor the specific entity) or the percentage of ownership interest held in CITIC Group Corporation by the Chinese government.[269] We also find inconsistencies between the records on file with the Commission and other publicly available information regarding the ultimate ownership of Pacific Networks and ComNet.[270] The Bureaus in the *Order to Show Cause* stated, "[t]he State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization, directly owns 100% of CITIC Group Corporation."[271] In support of this statement, the Bureaus cited to *pro forma* transfer of control notifications that were filed on behalf of Pacific Networks and ComNet in 2012.[272] However, the websites of the ultimate parent entity, CITIC Group Corporation, and an indirect parent entity, CITIC Limited, indicate that the Ministry of Finance (not the State-owned Assets Supervision and Administration Commission of the State Council) is the owner of CITIC Group Corporation.[273] The Ministry of Finance and the State-owned Assets Supervision and Administration Commission of the State Council appear to be different government entities with different leadership.[274] We find it unacceptable that Pacific Networks and ComNet failed to disclose this information given that the Commission is assessing the extent of control of the Chinese government. We again direct Pacific Networks and ComNet to provide the information required by the *Order to Show Cause* and to update the Commission's records, if needed.

58. Third, the *Order to Show Cause* directed Pacific Networks and ComNet to provide "an identification of all officers, directors, and other senior management officials of entities that hold ten percent or greater ownership interest in Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government."[275] Pacific Networks and ComNet provided this information for only Pacific Choice International Limited, the direct parent of Pacific Networks. The record indicates, however, that Pacific Networks and ComNet have other entities in their vertical chain of ownership that hold ten percent or greater ownership interest.[276] Instead of providing the requisite information for such entities, Pacific Networks and ComNet direct the Commission to look at the public record. They state, "the two public company entities in the ownership structure, CITIC Limited and CITIC Tel, are publicly traded companies listed on the Hong Kong Stock Exchange. As such, the identity

[268] Pacific Networks and ComNet Response at 10.

[269] *Id*., Exh. A.

[270] *See supra* para. 5 & notes 19, 20. Importantly, the PSI Report reflects that the "Chinese government" holds 100% direct interest in CITIC Group Corporation. PSI Report at 95; *id*. at note 607 ("The diagram is derived from information ComNet provided to the Subcommittee, as well as publicly available information."). The Executive Branch Letter is general in its language, as it refers to "CITIC Group Corporation ('CITIC'), a Chinese state-owned limited liability corporation" or "CITIC, a Chinese state-owned entity." Executive Branch Letter at 2, 11.

[271] *Order to Show Cause*, 35 FCC Rcd at 3735, para. 4.

[272] *Id*. at 3737, para. 9.

[273] *See supra* para. 5 & note 20.

[274] State-owned Assets Supervision and Administration Commission of the State Council, *About Us* http://en.sasac.gov.cn/aboutus.html (last visited Mar. 4, 2021); The State Council of the People's Republic of China, *Ministers*, http://english.www.gov.cn/statecouncil/202008/12/content_WS5f334b75c6d029c1c26379c3 html (last visited Mar. 4, 2021).

[275] *Order to Show Cause*, 35 FCC Rcd at 3737, para. 9.

[276] Pacific Networks and ComNet Response, Exh. A.

of their respective senior management personnel is a matter of public record (and is listed on those companies' respective websites) . . . ."[277] However, they do not provide citations to these websites. We do not find this answer to be responsive. Because Pacific Networks and ComNet have failed to fully respond to the *Order to Show Cause*, we again direct them to provide this information to the Commission and note that their prior response calls into question Pacific Networks' and ComNet's forthrightness.

59. Moreover, Pacific Networks and ComNet provided inconsistent statements about the corporate leadership of those entities concerning which they do present this information. Pacific Networks and ComNet certify "under penalty of perjury" that "Pacific Networks and ComNet are wholly-owned subsidiaries of Pacific Choice International Limited and that company's parent corporation, CITIC Telecom International Holdings Limited. Executives of their parent corporations do not participate in the daily operations of ComNet or Pacific Networks."[278] However, Exhibits B and C of their response shows that the two directors of Pacific Networks and ComNet are also Executive Directors of CITIC Tel.[279] One of these individuals is Chief Executive Officer of CITIC Tel, while the other individual is the Chief Financial Officer of CITIC Tel.[280] In addition to CITIC Tel, the two directors of Pacific Networks and ComNet are also directors of Pacific Choice International Limited.[281] These two individuals are the only persons identified in Pacific Networks' and Pacific Choice International Limited's corporate leadership.[282] Pacific Networks and ComNet further state that "[n]o other officers or senior officials are employed by Pacific Networks Corp."[283] and "[n]o other officers or senior officials are employed by Pacific Choice International Limited."[284] Pacific Networks' and ComNet's statements are inconsistent and further call into question Pacific Networks' and ComNet's forthrightness.

60. *Failure to File 2014 Pro Forma Notifications.* Pacific Networks and ComNet have admitted that they are not in compliance with the Commission's rules to file *pro forma* notifications for a *pro forma* transfer of control that occurred in 2014, but have yet to cure this deficiency. Pacific Networks and ComNet state that they "were alerted to the failure to file those notifications by the [*Order to Show Cause*], and are prepared to file such notifications on a *nunc pro tunc* basis or otherwise pending discussions with Commission staff on the best way to proceed."[285] Pacific Networks and ComNet admit that "a restructuring of the CITIC Group subsidiaries in 2014 resulted in a pro forma transfer of control of Pacific Networks and ComNet for which notifications of pro forma transfer were not filed under 47 C.F.R. §63.24(f)."[286] Pacific Networks and ComNet indicate that "a corporate restructuring occurred" and "[n]o material change of ultimate ownership was effected by this transaction," and after the transaction, "CITIC Group Corporation continued to control over 50% of CITIC Limited, and ultimately

[277] *Id*. at 12. Pacific Networks' and ComNet's failure to fully respond to the *Order to Show Cause*, or provide documentation of or citations to the "respective websites" of the two identified entities out of the "numerous" entities in their ownership structure, or certify that the information on the "respective websites" is responsive to the directive in the *Order to Show Cause*, raises troubling questions about their transparency and reliability.

[278] *Id*., Declaration of Li Ying (Linda) Peng.

[279] *Id*., Exhs. B, C.

[280] *Id*.

[281] *Id*.

[282] *Id*.

[283] *Id*., Exh. B.

[284] *Id*., Exh. C.

[285] *Id*. at 33.

[286] *Id*.

to control over 50% of Pacific Networks and ComNet."[287] According to Pacific Networks and ComNet, "[t]he net result of the 2014 transfer was to replace an aggregate 100% ownership link between CITIC Group and CITIC Limited with an aggregate ownership link of 58.13%" and "did not result in a change in the actual controlling party and is therefore considered non-substantial or *pro forma*."[288] Pacific Networks and ComNet add that they did not file a notification with the Commission, but did disclose the 2014 transaction to DOJ and DHS.[289] While Pacific Networks and ComNet informed the Executive Branch agencies, the Commission's rules required Pacific Networks and ComNet to timely file the *pro forma* notifications with the Commission.[290] It is the authorization holders' obligation to comply with the Commission's rules. Among other things, the Commission's *pro forma* rules ensure that the Commission and the public continue to have accurate and truthful information concerning international section 214 authorization holders. Pacific Networks' and ComNet's continued failure to file the *pro forma* notifications almost after seven years raises additional concerns as to whether the Commission and the U.S. government can trust Pacific Networks and ComNet to comply with U.S. law and regulations.

61. Overall, the record presents a troubling picture of Pacific Networks' and ComNet's lack of forthrightness in their response to the *Order to Show Cause*, based on a review of the record and the information that Pacific Networks and ComNet provided to the Senate Subcommittee as reflected in the PSI Report. We are unpersuaded by Pacific Networks' and ComNet's contention that they have "responded fully to the Bureaus' requests for information in the [*Order to Show Cause*] . . . ."[291] As described above, we have identified a number of instances where Pacific Networks and ComNet have not been transparent and forthright with the Commission. Pacific Networks and ComNet were required to provide accurate and truthful statements to the Commission. Their failure to respond truthfully and/or to provide critical information in response to the *Order to Show Cause* raises significant doubt as to whether Pacific Networks and ComNet can be trusted by the Commission and whether they can comply with the Commission's rules.

C. Termination of International Section 214 Authorizations

62. We next consider whether termination of Pacific Networks' and ComNet's international section 214 authorizations is warranted, separate and apart from revocation, based on Pacific Networks' and ComNet's record of compliance with the conditions in the International Bureau's grant of an international section 214 authorization to Pacific Networks and grant of a transfer of control of ComNet's international section 214 authorization to Pacific Networks. Under section 214(c) of the Act, the Commission "may attach to the issuance of the certificate such terms and conditions as in its judgment the public convenience and necessity may require."[292] Pacific Networks' and ComNet's two international section 214 authorizations, ITC-214-20090105-00006 and ITC-214-20090424-00199, are conditioned on the authorization holders abiding by the commitments and undertakings contained in their 2009 LOA.[293] The 2009 LOA provides that, "in the event the commitments set forth in this letter are breached, in addition to any other remedy available at law or equity, DHS or DOJ may request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization

[287] *Id*. at 6-7.

[288] *Id*. at 7.

[289] *Id*.

[290] 47 CFR § 63.24(f)(2) ("A *pro forma* assignee or a carrier that is subject to a *pro forma* transfer of control must file a notification with the Commission no later than thirty (30) days after the assignment or transfer is completed . . . .").

[291] Pacific Networks and ComNet Response at 37.

[292] 47 U.S.C. § 214(c).

[293] *Order to Show Cause*, 35 FCC Rcd at 3741-43, Appx. A, paras. 4, 6; 2009 LOA.

granted by the FCC to Pacific Networks, CM Tel, or any successor-in-interest to either."[294] Here, compliance with the commitments contained in the 2009 LOA was a material condition of the International Bureau's grant of the international section 214 authorization to Pacific Networks and grant of a transfer of control of ComNet's international section 214 authorization to Pacific Networks, and failure to comply with such commitments accordingly warrants consideration of termination of such authorizations.[295] Based on the record evidence, we believe Pacific Networks' and ComNet's compliance with the 2009 LOA should be examined closely to determine whether termination of their international section 214 authorizations is warranted.

63. The record evidence warrants a closer examination of the 2009 LOA given the apparent inconsistent statements made by Pacific Networks and ComNet to the Senate Subcommittee, the Executive Branch agencies, and the Commission. The provisions of the 2009 LOA include, for example: (1) "Pacific Networks and CM Tel agree to take all practicable measures to prevent unauthorized access to, or disclosure of the content of communications or U.S. records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in this letter;"[296] (2) "Pacific Networks and CM Tel agree that they will not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, Domestic Communications . . . to any person if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of DHS and DOJ or the authorization of a court of competent jurisdiction in the United States;"[297] and (3) "Pacific Networks and CM Tel agree to notify DHS and DOJ . . . of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter" and "of any material changes to their ownership structure."[298]

64. *Take All Practicable Measures to Prevent Unauthorized Access to U.S. Records*. From the record evidence, it is unclear whether U.S. records are stored only in the United States, Hong Kong, or both, and what, if any, practicable measures Pacific Networks and ComNet have taken under the 2009 LOA to prevent unauthorized access if U.S. records are in fact stored in Hong Kong or other non-U.S. locations and accessible by their direct or indirect parent companies. Our concern stems from the discrepancy reflected by the PSI Report, wherein ComNet informed the Senate Subcommittee in 2020 that its parent entities do not have direct access to U.S. records,[299] whereas records of Team Telecom's site visits noted that "ComNet used [CITIC Tel's] data center in Hong Kong as a back-up" and ComNet's "wholesale billing records 'are maintained in Hong Kong.'"[300] Based on these inconsistencies, we question where U.S. records are actually stored and what "practicable measures" Pacific Networks and

[294] 2009 LOA at 4.

[295] *See P & R Temmer v. FCC*, 743 F.2d 918 (D.C. Cir. 1984); *Atlantic Richfield Co. v. United States*, 774 F.2d 1193 (D.C. Cir. 1985); *see also Morris Communications, Inc. v. FCC*, 566 F.3d 184 (D.C. Cir. 2009) (automatic termination for non-payment did not violate administrative due process because in such situation "the licenses themselves . . . lapsed); *Alpine PCS, Inc. et al.*; *Requests for Waiver of the Installment Payment Rules and Reinstatement of Licenses*, Memorandum Opinion and Order, 25 FCC Rcd 469 (2010), *aff'd,* 404 Fed. Appx. 508 (D.C. Cir. 2010) (provision for automatic cancellation did not trigger section 312(a) revocation procedures).

[296] 2009 LOA at 2.

[297] *Id*. at 3.

[298] *Id*.

[299] PSI Report at 96 ("ComNet representatives informed the Subcommittee that its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems."); *id*. (stating that "its parent companies do not have direct access to these records and that they would need to request access from ComNet and follow ComNet's local procedures.").

[300] *Id*.

ComNet have taken in the past and are taking presently under the specific conditions of the 2009 LOA. Further, as noted above, {[

]}[302]

These concerns are particularly heightened in light of the national security and law enforcement concerns that the Executive Branch agencies have identified regarding Pacific Networks' and ComNet's retention of section 214 authority.

65. *Notification to Executive Branch Agencies of Location of U.S. Records and Access by Parent Entities.* Pacific Networks and ComNet agreed to notify DHS and DOJ "of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter."[303] In Pacific Networks' and ComNet's response to the *Order to Show Cause*, they provided the Commission with a redacted and unredacted letter from counsel for Pacific Networks and ComNet to Team Telecom dated July 6, 2015, in which counsel addresses {[

]}[304] They also provide a December 13, 2017 letter from counsel to Team Telecom which provides responses to a November 14, 2017 Team Telecom Inquiry, including information pertaining to {[

]}[306] If Pacific Networks and ComNet failed to inform the Executive Branch agencies of any material changes such as where U.S. records are currently located, that may constitute a violation of the 2009 LOA.

66. We seek clarity on this issue and therefore direct Pacific Networks and ComNet to verify for the Commission and the Executive Branch agencies whether Pacific Networks' and ComNet's statement to the Senate Subcommittee in 2020 that U.S. Records are only stored in the United States is accurate. If not, Pacific Networks and ComNet are directed to explain where all U.S. records are located and stored and describe in detail the "practicable measures" they have taken to prevent unauthorized access. Additionally, while noting that the Executive Branch agencies indicated that "[DOJ and DHS] have not identified acts of non-compliance,"[307] in preparation for any further filing the interested Executive Branch agencies may make, we encourage them to reexamine Pacific Networks' and ComNet's disclosures to the Senate Subcommittee and to the Commission in light of the 2009 LOA and describe in detail in any such filing any specific violations of the 2009 LOA that would provide additional context for the Commission's assessment as to whether it should terminate Pacific Networks' and ComNet's international section 214 authorities.

---

[301] Pacific Networks and ComNet Response, Exh. K at 21.

[302] *Id.*, Exh. K at 31; 2009 LOA at 2.

[303] 2009 LOA at 3.

[304] Pacific Networks and ComNet Response, Exh. K at 17-18.

[305] *Id.*, Exh. K at 19-24.

[306] *Id.* at 19-83.

[307] Executive Branch Letter at 10.

D. The Executive Branch Agencies State That Mitigation Measures Cannot Resolve National Security and Law Enforcement Concerns

67. We are not persuaded by Pacific Networks' and ComNet's argument that mitigation measures could address specific concerns about any security vulnerabilities.[308] The Executive Branch agencies, which have expertise in matters of national security and law enforcement and in monitoring carriers' compliance with risk mitigation agreements, have already provided their views on the national security risks posed by entities, like Pacific Networks and ComNet, that are owned and controlled by the Chinese government.[309] The agencies state that while Pacific Networks' and ComNet's international section 214 authorizations are conditioned on ongoing compliance with a 2009 Letter of Assurance with DOJ and DHS (together, the "Monitoring Agencies"), "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."[310]

68. Moreover, the Executive Branch agencies have assessed that additional mitigation measures are not appropriate because "the Chinese government's ownership and control over [Pacific Networks and ComNet] undermines [the Executive Branch agencies'] confidence that additional mitigation measures would effectively address the evolved law enforcement and national security risks. Put simply, mitigation requires a minimum level of trust, and that level of trust is absent here."[311] The Executive Branch agencies further state that 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 [Pacific Networks and ComNet] means that the Monitoring Agencies cannot rely on [Pacific Networks and ComNet] to self-report violations of more aggressive mitigation measures, especially if the Chinese government were to direct the Companies to violate those terms."[312]

69. As discussed above, based on their dealings with the Commission, we also have concerns regarding Pacific Networks' and ComNet's transparency and reliability, qualities that are relevant to a determination that the public interest is served by their retention of section 214 authority. As such, we similarly question Pacific Networks' and ComNet's ability to cooperate and be fully transparent with the Executive Branch agencies. In any event, consistent with our longstanding policy, we accord deference to the Executive Branch agencies' expertise in mitigating risks to national security and law enforcement and therefore are not persuaded by the argument that mitigation measures could address specific concerns about any security vulnerabilities in this case. We note that the process we adopt in this Order will provide Pacific Networks and ComNet and the Executive Branch agencies an additional opportunity to respond to this Order, and Pacific Networks and ComNet, the Executive Branch agencies, and the public sufficient time to provide input in the record, including the opportunity to seek leave to provide further evidence in light of future filings.

IV. PROCEDURAL MATTERS

70. *Written Submissions.* Pacific Networks Corp. (Pacific Networks) and ComNet (USA) LLC (ComNet) must submit a filing responding to the questions in Appendix A of this Order and demonstrate why the Commission should not revoke and/or terminate their section 214 authority no later than April 28, 2021. The public, including the Executive Branch agencies, may file a written response to

[308] Pacific Networks and ComNet Response at 31-32.

[309] *See generally* Executive Branch Letter.

[310] *Id*. at 2.

[311] *Id*. at 2, 10-12.

[312] *Id*. at 11.

the Response of Pacific Networks and ComNet to this Order no later than June 7, 2021. Pacific Networks and ComNet may file any additional evidence or arguments demonstrating why the Commission should not revoke and/or terminate their section 214 authority no later than June 28, 2021. All filings concerning matters referenced in this Order, including additional filings that may be submitted pursuant to the Commission's *ex parte* rules as set forth below, should refer to GN Docket No. 20-111.

71. *Ex Parte Presentations.* The proceeding this Order initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[313] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

72. *Filing Procedures.* Filings in this proceeding must be filed in the Commission's Electronic Comment Filing System (ECFS) in GN Docket No. 20-111.

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE Washington, DC 20554.
- Currently, the Commission does not accept any hand delivered or messenger delivered filings as a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. In the event that the Commission announces the lifting of COVID-19 restrictions, a filing window will be opened at the Commission's office located at 9050 Junction Drive, Annapolis, Maryland 20701.[314]

73. *People with Disabilities*: To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (TTY).

[313] 47 CFR §§ 1.1200 *et seq.*

[314] *Amendment of the Commission's Rules of Practice and Procedure*, Order, 35 FCC Rcd 5450 (OMD 2020).

74. *Contact Person*. For further information about this proceeding, please contact Gabrielle Kim, FCC International Bureau, 45 L Street, N.E., Washington, D.C. 20554, at (202) 418-0730 or Gabrielle.Kim@fcc.gov.

V. ORDERING CLAUSES

75. Accordingly, IT IS ORDERED that, pursuant to sections 4(i), 4(j), 214, 215, 218, and 403 of the Communications Act of 1934, as amended, and section 1.1 of the Commission's rules,[315] Pacific Networks Corp. and ComNet (USA) LLC MUST SUBMIT a filing responding to the questions in Appendix A and demonstrate why the Commission should not revoke and/or terminate their section 214 authority no later than **April 28, 2021**. The public, including the Executive Branch agencies, MAY FILE a written response to the Response of Pacific Networks Corp. and ComNet (USA) LLC to this Order no later than **June 7, 2021**. Subject to the provisions of this Order, Pacific Networks Corp. and ComNet (USA) LLC MAY FILE any additional evidence or arguments demonstrating why the Commission should not revoke and/or terminate their section 214 authority no later than **June 28, 2021**.

76. IT IS FURTHER ORDERED that a copy of this Order shall be sent by Certified Mail, Return Receipt Requested, and by regular first-class mail to:

Pacific Networks Corp. and ComNet (USA) LLC
c/o Jeffrey J. Carlisle
Stephen Coran
Rebecca Jacobs Goldman
David Burns
Jonathan Garvin
Lerman Senter LLP
2001 L Street NW, Suite 400
Washington, DC 20036

Linda Peng
General Manager, Human Resources & Administration
ComNet (USA) LLC
100 N. Barranca Street, Suite 910
West Covina, CA 91791

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

[315] 47 U.S.C. §§ 154(i), 154(j), 214, 215, 218, 403; 47 CFR § 1.1.

APPENDIX A

Further Request For Information

Pacific Networks and ComNet failed to fully respond to the *Order to Show Cause* and shall file a response with the Commission within forty (40) calendar days demonstrating why the Commission should not revoke and/or terminate their domestic and international section 214 authorizations. Pacific Networks and ComNet shall also include in their response the following information:

1. an identification of the Chinese government entity that owns and controls CITIC Group Corporation and the ownership interests held by such entity in CITIC Group Corporation;
2. a detailed description of the management and oversight of Pacific Networks and ComNet by any entity that holds a ten percent or greater **direct or indirect** ownership interest in and/or controls Pacific Networks and ComNet;
3. an identification of all officers, directors, and other senior management of all entities that hold a ten percent or greater **direct or indirect** ownership interest in and/or control Pacific Networks and ComNet, their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government;
4. a clarification whether ComNet is an LLC or a corporation as represented in certain filings before the Commission and, if necessary, explain in detail when a legal change occurred and whether Commission notification was required;
5. a description and copy of any policies or agreements concerning Pacific Networks' and ComNet's corporate governance or decision making;
6. with respect to U.S. customer records, provide: (1) an identification and description of the location(s) where U.S. customer records are stored, including original records, back-up records, and copies of original records; (2) a description and copy of any policies or agreements governing access to U.S. customer records; (3) an explanation and identification as to which entities and individuals have access to U.S. customer records, how such access is granted, and any corporate policies concerning such access;
7. a description of who has access to the servers and/or data centers where U.S. customer records are located and any policies, agreements, or standards concerning access to the servers or data centers where U.S. customer records are stored;
8. a detailed response as to whether any U.S. records are stored or were ever stored in CITIC Tel's data center in Hong Kong or in other non-U.S. locations, identifying the data center, its location, the time frame, and the type of service;
9. a detailed description of previous and present "practicable measures" taken to prevent unauthorized access to U.S. records as required by the 2009 LOA;
10. a detailed description of what, if any, practicable measures Pacific Networks and ComNet have taken under the 2009 LOA to prevent unauthorized access if U.S. records are in fact stored in Hong Kong or other non-U.S. locations and accessible by their direct or indirect parent companies or other third parties;
11. a detailed description as to whether Pacific Networks and ComNet failed to inform the Executive Branch agencies "of any material changes in any of the facts as represented in [the 2009 LOA], or in notices or descriptions submitted pursuant to this letter," as required by the 2009 LOA.
12. a description and copy of any policies and/or procedures in place to protect personally identifiable information (PII) and customer proprietary network information (CPNI);

13. a description of any domestic interstate communications services that have been provided, are provided, and/or will be provided in the near future pursuant to Pacific Networks' and ComNet's blanket domestic section 214 authority as described in section 63.01 of the Commission's rules, 47 CFR § 63.01;
14. a description of any services that have been provided, are provided, and/or will be provided in the near future pursuant to the international section 214 authorities granted to Pacific Networks and ComNet;
15. a detailed description of Pacific Networks' and ComNet's domestic communications infrastructure within the United States and its connectivity to operations infrastructure within Hong Kong and China and provide a copy of what Pacific Networks and ComNet provided to DOJ as identified in a June 8, 2018 letter from DOJ to Pacific Networks and ComNet;[1]
16. a detailed response that explains: (1) what Autonomous System numbers have been assigned and deployed for the IP networks of Pacific Networks and ComNet; (2) whether Border Gateway Protocol (BGP) routers are used to exchange routing updates to forward IP traffic between these (i.e., Pacific Networks' and ComNet's) networks, or whether an Interior Gateway Protocol (IGP) routing protocol (e.g., OSPF or IS-IS) is used to forward IP traffic between these networks; and (3) if BGP is used, whether Pacific Networks and ComNet directly peer BGP speakers with no intermediate third party BGP routing provider connecting both networks;
17. a detailed response that explains, {[

]}
18. an identification of Pacific Networks' peering relationships with other U.S. providers at the Points of Presence (PoP) located in the United States[3]
19. a detailed response that explains the discrepancies and/or omissions, as described in this Order, concerning: (1) ComNet's statements to the Senate's Permanent Subcommittee on Investigations, as described in the PSI Report, and the statements made by Pacific Networks and ComNet in response to the *Order to Show Cause*; and (2) if statements made to the Commission were not accurate and complete when filed, provide accurate and complete responses to explain the discrepancies and/or omissions and to ensure the Commission has all relevant information to conduct its assessment;
20. an identification of the percentage of calls using IDD service that use SS7 compared to SIP based Interconnected VoIP;
21. an identification of the percentage of A2P messages that are sent through IP based networks versus SS7;
22. a detailed description of the measures to ensure privacy and integrity of data stored in ComNet's facilities supporting current and near future section 214 authority services.
23. {[

[1] Pacific Networks and ComNet Response, Exh. K at 156-157.

[2] *Id.*, Exh. K at 24.

[3] *Id.*, Exh. D at D-1.

]}[4]

24. {[
]}[5]
25. copies of the letters sent to the Commission confirming implementation of both ISPCs (3-193-4 and 3-191-6);
26. an explanation as to whether both ISPCs (3-193-4 and 3-191-6) have been in continuous use since their implementation;
27. an explanation of why ComNet needs two ISPCs for the {[
]};[6]
28. an explanation concerning whether the Traffic and Revenue reports submitted for the years 2003-2014 reflected use of one or both of these ISPCs;
29. an explanation as to why Traffic and Revenue reports were not submitted for the years 2003, 2005, and 2007;
30. an explanation as to whether Pacific Networks and ComNet filed with the Commission corrected versions of the *pro forma* transfer of control notifications originally filed with the Commission on January 26, 2012, that they provided to DHS and DOJ on February 16, 2012;[7] and if corrected versions of the *pro forma* transfer of control notifications were not filed with the Commission, Pacific Networks and ComNet shall file the corrected *pro forma* notifications in IBFS; and
31. a complete description of all work required for Pacific Networks and ComNet to discontinue all section 214 services to their customers if the Commission were to revoke and/or terminate Pacific Networks' and ComNet's section 214 authorities, along with a detailed estimate of the time required for each portion of that work and an explanation of how that estimate was reached.

[4] *Id*., Exh. K at 42.

[5] *Id.*, Exh. K at 49.

[6] *Id*. at 16.

[7] *Id.*, Exh. K at 68-71.

STATEMENT OF
ACTING CHAIRWOMAN JESSICA ROSENWORCEL

Re: *China Unicom (Americas) Operations Limited,* GN Docket No. 20-110, ITC-214-20020728-00361, ITC-214-20020724-00427;
Pacific Networks Corp. and ComNet (USA) LLC, GN Docket No. 20-111, ITC-214-20090105-00006, ITC-214-20090424-00199.

In the United States, we have long recognized that the free flow of information across borders and between countries is vital to our economic growth and vibrancy. That is why the Federal Communications Commission has a history of working to open American markets to foreign telecommunications companies, when doing so is in the public interest. More often than not, these connections make us stronger because they help us share our democratic values with the rest of the world.

But not all connections are in the United States' national security interest. We know some countries may seek to exploit our openness to advance their own national interests. And when we cannot mitigate that risk, we need to take action to protect the networks that are important to our national security and economic prosperity.

That is what we do today. We institute proceedings to revoke the domestic authority and international authorizations issued to three companies: China Unicom Americas, Pacific Networks, and ComNet. The evidence compiled in our proceedings confirms that these companies are indirectly owned and controlled by the Chinese government. As a result, there is strong reason to believe that they will have to comply with requests from the Chinese government and advance its goals and policies. Moreover, Executive Branch agencies have concluded that mitigation measures would not be able to address the significant national security and law enforcement concerns raised here.

The actions we take today are consistent with our 2019 decision to deny China Mobile USA's application for FCC authorization. They are consistent with our 2020 decision to start a proceeding to revoke China Telecom Americas' prior authorization to provide service within the United States.

They are also just the start of what needs to be a more comprehensive effort to periodically review authorization holders with foreign ownership providing service in the United States. After all, last year a bipartisan report from the Senate Permanent Subcommittee on Investigations detailed how the federal government has provided almost no oversight of Chinese state-owned telecommunications companies for nearly twenty years.

It's time to fix this. Here's how we will do so.

First, I have directed the agency's International Bureau to look back at this agency's past grants of international Section 214 applications and recommend options for addressing evolving national security risks.

Second, because we rely on our peers in the Executive Branch to assess national security and law enforcement concerns, I have offered the FCC's help in establishing a process to periodically review international Section 214 authorizations that raise national security risks.

Third, because the concerns we address today also apply to applications for submarine cable landing licenses, I have directed the International Bureau to continue to refer these applications to the Executive Branch agencies for review. On that front, I am pleased that applicants to build a Trans-Pacific cable linking Hong Kong to California agreed last week to reconfigure that system to meet ongoing national security concerns.

This is progress, as are the decisions adopted here today. They positively reflect both our values and our need for security. A big thank you to the agency staff who worked on this effort, including Stacey Ashton, Denise Coca, Kathleen Collins, Francis Gutierrez, Jocelyn Jezierny, David Krech,

Gabrielle Kim, Arthur Lechtman, Wayne Leighton, Ron Marcelo, Adrienne McNeill, Thomas Sullivan, and Troy Tanner from the International Bureau; Doug Klein, Jacob Lewis, Scott Noveck, Joel Rabinovitz, and Bill Richardson from the Office of General Counsel; Pamela Arluk, Jodie May, and Terri Natoli from the Wireline Competition Bureau; Pamela Kane and Christopher Killion from the Enforcement Bureau; Kenneth Carlberg, Jeffery Goldthorp, Debra Jordan, and Lauren Kravetz from the Public Safety and Homeland Security Bureau; Eric Burger, Robert Cannon, Marilyn Simon, Virginia Metallo, and Emily Talaga from the Office of Economics and Analytics; as well as Padma Krishnaswamy from the Office of Engineering and Technology.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427;
Pacific Networks Corp. and ComNet (USA) LLC, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199.

As we move toward a more interconnected future, the Commission must protect the integrity of our networks. Today, we take another important step in ensuring American networks are guarded against adversary state-owned or controlled carriers by initiating a proceeding to revoke the authority of China Unicom Americas, Pacific Networks and its wholly owned subsidiary, ComNet, to operate in the United States.

Today's decisions further our commitment to preserving the safety and security of our communications. Over the last two years, the Commission has rejected an application from the U.S. subsidiary of China Mobile, the largest mobile provider in the world, and initiated a proceeding to revoke U.S. operating authority from China Telecom Americas, the U.S. subsidiary of China's largest telecom provider. Like those carriers, the companies that are the subject of today's actions are ultimately owned and/or controlled by the Chinese government and therefore vulnerable to its exploitation and control, creating a significant threat to our national security and law enforcement interests.

These companies are required under Chinese law to disclose sensitive customer information upon demand to assist government intelligence activities. They've also demonstrated a lack of transparency and reliability in previous dealings with the Commission and Team Telecom. For example, both companies failed to comply with Commission rules concerning disclosure of ownership changes and company reorganization, and they failed to provide crucial information concerning their affiliations with the Chinese government and cybersecurity practices. According to Team Telecom, there are no mitigation measures that could enable the companies' continued operation in the United States.

Our actions represent a bipartisan consensus across the federal government that American communications must be protected from companies owned or controlled by the Chinese government. Our responsibilities don't stop at the border. As I stated last year, international undersea cables carry 99% of the world's data traffic, and Chinese companies and their American partners are actively seeking to increase the number of cables connecting our countries. As we saw with the withdrawal of an undersea cable application just one week ago connecting California and Hong Kong, however, applicants are coming to understand that the Commission and its federal partners will not approve any application that fails to guarantee the fundamental security of American communications from any tampering, blocking, or interception by adversary states or other bad actors.

All of these issues highlight another security threat to our communications and privacy. Even as we act to remove or block Chinese telecom carriers from accessing U.S. networks, many of these same companies also own data centers operating within the United States, including multiple locations in metro areas like the Washington, DC area, New York City, and Los Angeles.[1] As the Department of Homeland Security has warned, these data centers leave their customers vulnerable to data theft for one of the same reasons we act today – Chinese law requires these companies to secretly share data with the Chinese government or other entities upon request, even if that request is illegal under U.S. law.[2] Currently, the

[1] *See, e.g.,* China Telecom Data Center Locations, https://www.datacenters.com/china-telecom-data-center-locations (last visited Mar. 12, 2021).

[2] *See* U.S. Dept. of Homeland Security, Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China (rel. Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

FCC lacks the authority to address this potential national security threat, but as part of any review of our jurisdiction over broadband services generally, the Commission should work with the new Administration and Congress to consider whether the FCC needs broader jurisdiction to tackle this emerging network security issue as well.

Thank you to the staff of the International Bureau for their work on these items.