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

In the Matter of	)	
	)	
China Unicom (Americas) Operations Limited	)	GN Docket No. 20-110;
	)	ITC-214-20020728-00361;
	)	ITC-214-20020724-00427
	)	
	)	
	)	

ORDER ON REVOCATION

Adopted: January 27, 2022 **Released: February 2, 2022**

By the Commission: Chairwoman Rosenworcel and Commissioners Carr and Starks issuing separate statements.

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 3
III. DISCUSSION 20
A. Standard of Review 21
1. Commission Authority 21
2. Applicable Standard of Proof 25
3. Public Interest Standard 27
4. CUA Had Sufficient Notice and Several Opportunities to Be Heard 29
B. Revocation of Section 214 Authority 49
1. The Chinese Government Indirectly Owns and Controls CUA 50
2. CUA's Retention of Section 214 Authority Presents National Security and Law Enforcement Risks 74
3. CUA's Past Representations to the Commission and Congress Support Revocation of its Section 214 Authority 111
C. Mitigation Would Not Address National Security and Law Enforcement Concerns 124
D. Transition Period 130
IV. ORDERING CLAUSES 135

I. INTRODUCTION

1. In this Order on Revocation (Order), we revoke China Unicom (Americas) Operations Limited's (CUA) domestic and international authority, pursuant to section 214 of the Communications Act of 1934, as amended (Act).[1] Based on our public interest analysis under section 214 of the Act and

[1] 47 U.S.C. § 214; *China Unicom (Americas) Corporation*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, Order to Show Cause, 35 FCC Rcd 3721 (IB, WCB, EB 2020) (*Order to Show Cause*); *China Unicom (Americas) Corporation*, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, Order Instituting Proceeding on Revocation, 36 FCC Rcd 6319 (2021) (*Institution Order*);
(continued….)

the totality of the record, we find that the present and future public interest, convenience, and necessity is no longer served by CUA's retention of its section 214 authority.

2. First, we find that CUA, a U.S. subsidiary of a Chinese state-owned enterprise, is subject to exploitation, influence, and control by the Chinese government, and is highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight. Second, given the changed national security environment with respect to China since the Commission authorized CUA to provide telecommunications services in the United States, we find that CUA's ties to the Chinese government—together with Chinese laws obligating CUA and its direct and indirect parent entities to cooperate with requests by the Chinese government—pose a clear and imminent threat to the security of the United States due to CUA's access to U.S. telecommunications infrastructure. Third, independent of these concerns, CUA's conduct and representations to the Commission and Congress demonstrate a lack of candor, trustworthiness, and reliability that erodes the baseline level of trust that the Commission and other U.S. government agencies require of telecommunications carriers given the critical nature of the provision of telecommunications service in the United States. Fourth, given the record evidence, we find that mitigation would not address these significant national security and law enforcement concerns. We therefore revoke CUA's domestic and international section 214 authority. Accordingly, we direct CUA to discontinue any domestic or international services that it provides pursuant to its section 214 authority no later than sixty (60) days from the release of this Order.

II. BACKGROUND

3. A complete procedural history leading to our adoption of the *Institution Order* on March 17, 2021 is discussed in detail therein.[2] As we stated in the *Institution Order,* 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 . . . ."[3] Promotion of national security is an integral part of the Commission's public interest responsibility, including its administration of section 214 of the Act, and indeed one of the core purposes for which Congress created the Commission.[4] The Commission has taken a number of targeted steps to protect the nation's communications infrastructure from potential security threats,[5] and we continue to do so here.

(Continued from previous page)
China Unicom (Americas) Operations Limited, Response to Order to Show Cause, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427 (June 1, 2020) (CUA Response to *Order to Show Cause*) (filing with the Commission a public filing and a non-public business confidential filing); China Unicom (Americas) Operations Limited, Response to Order Instituting Proceeding on Revocation, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427 (Apr. 28, 2021) (CUA Response to *Institution Order*) (filing with the Commission a public filing and a non-public business confidential filing).

[2] *See Institution Order*, 36 FCC Rcd at 6324-28, paras. 8-14.

[3] 47 U.S.C. § 151; *Institution Order*, 36 FCC Rcd at 6320, para. 2 (quoting 47 U.S.C. § 151); *see China Telecom (Americas) Corporation*, GN Docket No. 20-109, ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Order on Revocation and Termination, FCC 21-114, 2021 WL 5161884 (adopted Oct. 26, 2021 and released Nov. 2, 2021) (*China Telecom Americas Order on Revocation and Termination*); *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 (2019) (*Protecting Against National Security Threats Order*), *aff'd*., *Huawei Technologies USA, Inc. v. FCC*, 2 F.4th 421, 439 (5th Cir. 2021).

[4] 47 U.S.C. § 151; *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*); *see also Protecting Against*
(continued….)

4. 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 . . . ."[6] 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.[7] 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.[8] 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 an international section 214

(Continued from previous page)
National Security Threats Order, 34 FCC Rcd at 11436, para. 34, *aff'd. Huawei Technologies USA v. FCC,* 2 F.4th at 439.

[5] *See, e.g.*, *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, 3365-66, 3376-77, 3380, paras. 8, 31-32, 38 (2019) (*China Mobile USA Order*); *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, paras. 26-27; *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7822, paras. 2-3 (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. 1 (2020) (*Protecting Against National Security Threats Second Report and Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Third Report and Order, FCC 21-86, (rel. July 14, 2021); *Institution Order*, 36 FCC Rcd at 6320, para. 2; *China Telecom Americas Order on Revocation and Termination*.

[6] 47 U.S.C. § 214(a) (emphasis added); *see 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, para. 2, n.2 (2014) ("Any party seeking to provide common carrier telecommunications services between the United States, its territories or possessions, and a foreign point must request authority by application pursuant to section 214(a) of the Act, 47 U.S.C. § 214(a), and section 63.18 of the Commission's rules, 47 C.F.R. § 63.18.") (*ECO Test Report and Order*). 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 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 Order*).

[7] *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.

[8] *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.

authorization for revocation based on public interest considerations.[9] Based on public interest considerations, the Commission has initiated revocation proceedings and revoked section 214 authorizations in a variety of contexts.[10]

5. 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 considered 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.[11] With regard to this factor, the Commission has sought the expertise of the relevant Executive Branch agencies[12] for almost 25 years, and has accorded deference to their expertise in

[9] *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 World Trade Organization (WTO) carrier and such affiliation poses a very high risk to competition that cannot be remedied by safeguards); *id*., 15 FCC Rcd 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); *ECO Test Report and Order*, 29 FCC Rcd at 4259, 4266, paras. 6, 22 (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).

[10] *See, e.g.*, *Institution Order*, 36 FCC Rcd 6319; *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 (2020) (*China Telecom Americas Institution Order*); *Pacific Networks Corp. and ComNet (USA) LLC*, GN Docket No. 20-111, File Nos. ITC-214-20090105-00006, ITC-214-20090424-00199, Order Instituting Proceeding on Revocation and Termination, 36 FCC Rcd 6368 (2021) (*Pacific Networks/ComNet Institution Order*); *CCN, Inc. et al.,* Order to Show Cause and Notice of Opportunity for Hearing, 12 FCC Rcd 8547 (1997) (*CCN, Inc. Order to Show Cause*); *CCN, Inc. et al.,* Order, 13 FCC Rcd 13599 (1998) (*CCN, Inc. Order*) (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-TCD & WCB-CPD 2017).

[11] *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, 10962-64, paras. 90-92 (2020) (*Executive Branch Process Reform Report and Order*).

[12] 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. 20-110, File Nos. ITC-

(continued….)

identifying such a concern.[13] The Commission has formalized the review process for the Executive Branch agencies to complete their review consistent with Executive Order No. 13913 of April 4, 2020 that established the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee).[14] The Commission ultimately makes an independent 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.[15]

6. *CUA's Section 214 Authority*. CUA is authorized to provide domestic interstate telecommunications service pursuant to blanket section 214 authority that the Commission has issued by rule.[16] CUA holds two international section 214 authorizations, ITC-214-20020728-00361 and ITC-214-20020724-00427, both of which were originally granted in 2002.[17]

7. CUA is a California corporation that is headquartered in Virginia.[18] CUA is indirectly and ultimately owned and controlled by the Chinese government.[19] CUA is the wholly owned subsidiary

(Continued from previous page)
214-20020728-00361, ITC-214-20020724-00427) (Executive Branch Letter). DOJ, DHS, and DOD also are known informally as "Team Telecom."

[13] *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.

[14] *See generally Executive Branch Process Reform Report and Order*; Executive Order No. 13913 (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 (DOD), the Secretary of Homeland Security (DHS), and the Attorney General of the Department of Justice (DOJ), who serves as the Chair, and the head of any other executive department or agency, or any Assistant to the President, 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 (USTR)).

[15] *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.").

[16] 47 CFR § 63.01.

[17] On September 11, 2002, the International Bureau granted China Netcom (USA) Operations Limited (China Netcom USA) an international section 214 authorization, ITC-214-20020728-00361, to provide global or limited global facilities-based and resale service, subject to dominant carrier regulation on the U.S.-China route. On September 27, 2002, the International Bureau granted China Unicom USA LLC an international section 214 authorization, ITC-214-20020724-00427, to provide global or limited global facilities-based and resale service, subject to dominant carrier regulation on the U.S.-China route. On June 12, 2003, the International Bureau issued a Public Notice of a *pro forma* assignment of that authorization from China Unicom USA LLC to China Unicom USA Corporation (China Unicom USA). CUA Response to *Institution Order* at 32. As a result of several subsequent *pro forma* assignments and transfers of control—including the merger of China Netcom USA into China Unicom USA and the latter changing its name to CUA—CUA became the holder of the two international section 214 authorizations. A detailed description of the history of CUA's international section 214 authorizations is contained in the *Order to Show Cause*. *Order to Show Cause*, 35 FCC Rcd at 3728-31, Appx. A.

[18] *Institution Order*, 36 FCC Rcd at 6323, para. 5; CUA Response to *Institution Order* at 32; CUA Response to *Order to Show Cause* at 9, 16, 18-19, 30; *Order to Show Cause*, 35 FCC Rcd at 3722-23, para. 4. According to
(continued….)

of China Unicom Global Limited (CUG), an entity registered and established in Hong Kong.[20] CUG is wholly owned by China Unicom (Hong Kong) Limited (CUHK), an entity incorporated in Hong Kong and listed on the Hong Kong Stock Exchange (HKSE).[21] According to its SEC filings, CUHK is indirectly controlled by China United Network Communications Group Company Limited (CU),[22] an

(Continued from previous page)
CUA, CUA was formed as a limited liability company in California on May 24, 2002 and CUA converted into a corporation on April 17, 2003. CUA Response to *Institution Order* at 32; CUA Response to *Order to Show Cause* at 16.

[19] *Institution Order*, 36 FCC Rcd at 6323, para. 5; CUA Response to *Institution Order* at 31-33; CUA Response to *Order to Show Cause* at 16-18; *Order to Show Cause*, 35 FCC Rcd at 3722-23, para. 4; *see also* China Unicom (Americas) Operations Limited, Notification of Pro Forma Transfer of Control of International Section 214 Authorizations and Cable Landing License, File No. ITC-T/C-20170301-00025, Attach. 1 at 2 (Mar. 1, 2017) (stating that "the [People's Republic of China] government continues to maintain ownership and control over CUA and will continue to do so.") (2017 *Pro Forma* Notification).

[20] *Institution Order*, 36 FCC Rcd at 6323, para. 5; CUA Response to *Institution Order* at 32; CUA Response to *Order to Show Cause* at 16-17; *Order to Show Cause*, 35 FCC Rcd at 3722-23, para. 4.

[21] *Institution Order*, 36 FCC Rcd at 6323, para. 5; CUA Response to *Institution Order* at 32; CUA Response to *Order to Show Cause* at 16-18; *Order to Show Cause*, 35 FCC Rcd at 3722-23, para. 4. CUHK was previously listed on the New York Stock Exchange (NYSE). *Institution Order*, 36 FCC Rcd at 6323, para. 5; CUA Response to *Institution Order* at 32; CUA Response to *Order to Show Cause* at 16-18; *Order to Show Cause*, 35 FCC Rcd at 3722-23, para. 4 (noting that CUHK was also listed on the New York Stock Exchange (NYSE)). On January 6, 2021, the NYSE announced the NYSE Regulation's decision to delist CUHK along with China Telecom Corporation Limited, and China Mobile Limited, effective January 11, 2021. *See* Press Release, Intercontinental Exchange, NYSE Announces Suspension Date for Securities of Three Issuers and Proceeds with Delisting (Jan. 6, 2021), https://ir.theice.com/press/news-details/2021/NYSE-Announces-Suspension-Date-for-Securities-of-Three-Issuers-and-Proceeds-with-Delisting/default.aspx. Following an appeal and a decision affirming the prior determination, NYSE filed Form 25 with the U.S. Securities and Exchange Commission, in regard to each company, on May 7, 2021. *See* Chong Koh Ping and Alexander Osipovich, *NYSE to Delist Chinese Telecom Carriers After Rejecting Appeals* (May 7, 2021), https://www.wsj.com/articles/nyse-to-delist-chinese-telecoms-carriers-after-rejecting-appeals-11620394719; U.S. Securities and Exchange Commission, Form 25 – Notification of Removal from Listing and/or Registration under Section 12(b) of the Securities Exchange Act of 1934 (Form 25) (Issuer: CHINA TELECOM CORP LTD) (filed May 7, 2021), https://go.usa.gov/x6RKs; U.S. Securities and Exchange Commission, Form 25 (Issuer: CHINA MOBILE LTD /ADR/) (filed May 7, 2021), https://go.usa.gov/x6Rkx; U.S. Securities and Exchange Commission, Form 25 (Issuer: CHINA UNICOM (HONG KONG) Ltd) (filed May 7, 2021), https://go.usa.gov/xMdDd. *See also* Executive Order 13959 of Nov. 12, 2020, Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies, 85 Fed. Reg. 73185 (Nov. 17, 2020) (including "CHINA UNICOM (HONG KONG) LIMITED" among companies designated as a "Communist Chinese military company").

[22] Shares of CUHK are held by China Unicom Group Corporation (BVI) Limited (CUG BVI) (26.4%), China Unicom (BVI) Limited (CU BVI) (53.5%), and public shareholders (20.1%). CUG (BVI)'s equity is 100% held by CU. CUA Response to Institution Order at 31-32. CU (BVI) is owned as follows: CU (17.9% equity) and China United Network Communications Limited (CU A-Share), a public company listed on the Shanghai Stock Exchange (82.1% equity). Id. at 32-33. CUA states that as of April 2021, CU A-Share's shareholders are: (1) CU (36.8%) and (2) a group of strategic investors (Strategic Investors), public shareholders, and employee restricted incentive shares (63.2%). Id. at 33. CUA has not identified any other 10% or greater owners. Although CUA states that CU holds 36.8% of CU A-Share, in CUHK's 2020 annual filing with the Securities and Exchange Commission (SEC), CUHK states that "[CU] indirectly controlled an aggregate of approximately 79.9% of our issued share capital as of April 15, 2020." Id. at 33; China Unicom (Hong Kong) Limited, Annual Report (Form 20-F) at 13 (Apr. 22, 2020) (2020 CUHK SEC Annual Report). CUHK states that "[a]s our ultimate controlling shareholder, subject to our articles of association and applicable laws and regulations, [CU] is effectively able to control our management, policies and business by controlling the composition of our board of directors and, in turn, indirectly controlling the selection of our senior management, determining the timing and amount of our dividend payments, approving significant corporate transactions, including mergers and acquisitions, and approving our annual budgets." 2020 CUHK SEC Annual Report at 13; id. at Exh. 4.73, Integrated Service Agreement 2020-2022 between China United Network

(continued….)

entity incorporated in the People's Republic of China.[23] All of CU's shares are held by the State-owned Assets Supervision and Administration Commission of the State Council (SASAC), a Chinese government organization.[24]

8. *Pro Forma Notification.* On September 8, 2021, CUA filed a notification of a *pro forma* transfer of control, following the request of the International Bureau, Wireline Competition Bureau, and Enforcement Bureau (the Bureaus) that CUA explain "whether certain *pro forma* transfer of control actions occurred between 2009 and 2017 concerning the subject international section 214 authorizations."[25] Pursuant to section 63.24(f) of the Commission's rules, notifications must be filed within thirty (30) days after the transfer is completed.[26] In its filing, CUA states that control of its international section 214 authorizations was transferred from CUHK to CUHK's wholly owned subsidiary Billion Express Investments Co., Ltd (Billion), as part of an internal restructuring on December 30, 2011.[27] CUA states that Billion "became the direct owner of CUA," but it "did not change the ultimate ownership or control of CUA."[28] CUA added that it filed a *pro forma* transfer of control notification on March 1, 2017, when the ownership of CUA was transferred from Billion to CUG,[29] and Billion was dissolved on April 25, 2017.[30]

9. *CUA's Section 214 Services.* CUA states that with regard to domestic interstate telecommunications services,[31] it "has provided, or currently provides, the following telecommunications

(Continued from previous page)
Communications Group Company Limited and China United Network Communications Corporation Limited at 2 (October 21, 2019) (CUHK states that "[CU] is the controlling shareholder of [CU A-Share]"). More recently, in its 2021 SEC Annual Report, CUHK states that "[a]s of April 14, 2021, our ultimate controlling shareholder, [CU], through its 17.9% direct interest in [CU BVI], 36.8% direct interest in [CU A-Share] (which in turn holds 82.1% of [CU BVI]) and 100% direct interest in [CUG BVI], indirectly controlled approximately 24.5 billion shares of [CUHK], or 79.9% of our total outstanding shares." China Unicom (Hong Kong) Limited, Annual Report (Form 20-F) at 72 (Apr. 21, 2021) (2021 CUHK SEC Annual Report). Further, according to the 2021 CUHK SEC Annual Report, eight of CUHK's twelve directors and executive officers also held positions on both CU and CU A-Share's board of directors and/or senior management. *Id*. at 65-67.

[23] CUA Response to *Institution Order* at 33 ("[CU] was incorporated in Beijing on June 18, 1994").

[24] *Id*. & n.122.

[25] *Order to Show Cause*, 35 FCC Rcd at 3726, para. 9; *see* China Unicom (Americas) Operations Limited, IBFS File No. ITC-T/C-20210908-00128, *Notification of Pro Forma Transfer of Control of International Section 214 Authorizations*, (Sept. 8, 2021) (2021 *Pro Forma* Notification); *see also infra* para. 12. In its notification, CUA states that "[a]s part of an internal reorganization control of CUA was transferred from [CUHK] to its wholly-owned subsidiary Billion on December 30, 2011. Billion therefore became the new immediate parent of CUA." 2021 *Pro Forma* Notification, Attach. at 3.

[26] 47 CFR § 63.24(f).

[27] 2021 *Pro Forma* Notification, Attach. at 3.

[28] *Id*. at 1. *See also id*. at 6 ("CUA certifies that the transaction was pro forma and that, together with all previous pro forma transactions, did not result in a change in the ultimate controlling party.")

[29] *Id*. at 2. *See generally* 2017 *Pro Forma* Notification. CUA's 2017 filing states that, "[a]s a result of the restructuring steps, CUG, a company that is ultimately owned and controlled by the People's Republic of China ('PRC'), became the direct owner of CUA. The restructuring did not change the ultimate ownership or control of CUA as the PRC government continues to maintain ownership and control over CUA and will continue to do so." *Id*. at 1-2.

[30] 2021 *Pro Forma* Notification, Attach. 3 at 2.

[31] CUA notes that "[a] section 214 authorization is required by any company that provides telecommunications on a common carrier basis." CUA Response to *Order to Show Cause* at 24 (citing 47 U.S.C. § 214). CUA also cites to 47 U.S.C. § 153(50) for the definition of "telecommunications," § 153(53) for the definition of "telecommunications service," and § 153(11) for the definition of "common carrier" or "carrier." *Id.* at 24, n.50.

services:" Dedicated Private Line circuits, Ethernet Private Line (EPL), and MVNO services.[32] With regard to U.S.-international telecommunication services, CUA states that it "has provided, or currently provides," the following telecommunications services: Private Leased Circuit (IPLC), EPL (IEPL), MVNO, and International Wholesale Voice.[33] Based on its filings, with the exception of International Wholesale Voice services, which CUA states were terminated in the third quarter of 2017,[34] CUA appears to currently offer the above services pursuant to its section 214 authority.[35]

10. CUA states that it also provides the following services that it considers "'information' or other non-telecommunications services": Multi-protocol Label Switching Virtual Private Network (MPLS VPN) services, IP Transit services, Smart Video Network (SVN) services, Dedicated Internet Access (DIA) services, Data Center services, Cloud Services, and Resold Services, which include the resale of dark fiber, data center services, and system integration offered by CUA's local partners.[36] CUA also states that in the event the Commission revokes CUA's section 214 authorizations, "it believes that other than the MVNO services, it can continue to provide all of its remaining services on a private carriage basis, without a section 214 authorization."[37]

11. *Order to Show Cause*. On April 24, 2020, the Bureaus issued the *Order to Show Cause* directing CUA to file a response within thirty (30) calendar days demonstrating why the Commission should not initiate a proceeding to revoke CUA's domestic and international section 214 authorizations.[38]

---

[32] CUA Response to *Institution Order* at 44 (listing Dedicated Private Line circuits and EPL under the category of reselling "local partners' services to our end use customers"); *see infra* paras. 75, 77 & note 363. CUA states that "to the extent these telecommunications services are or were *domestic* interstate telecommunications services, provided by CUA on a *common carrier basis*, CUA provides or has provided them pursuant to its blanket domestic section 214 authorization." CUA Response to *Institution Order* at 44 (emphasis in original). Although, as noted above, CUA appears to concede that all of these services are "telecommunications services" as defined in section 3(53) of the Communications Act, it then asserts that except for its MVNO services, "CUA provides all of its other telecommunication services pursuant to individually tailored and negotiated contracts." *Id.* at 44-45, n.147.

[33] CUA Response to *Institution Order* at 45-46; *id*. at 46 ("In the past CUA's [International Wholesale Voice] service provided International Voice Termination premium quality routes and Tier 1 services with both fixed and mobile operators operating in different regions of the world. CUA terminated this service offering in the third quarter of 2017."); *see infra* paras. 75, 77 & note 363. CUA states that "[t]o the extent these telecommunications services were or are *U.S.-international* telecommunications services, provided by CUA on a *common carrier basis*, CUA has provided or currently provides them pursuant to its international section 214 authorizations." CUA Response to *Institution Order* at 46 (emphasis in original); *id*. at 44-45, n.147. CUA further states that given the current uncertainties surrounding the future of its section 214 authorizations, it presently has no plans to launch new domestic or U.S.-international services on a common carrier basis. *Id.* at 44-46.

[34] CUA Response to *Institution Order* at 46.

[35] CUA Response to *Order to Show Cause* at 24-25.

[36] *Id*. In response to the *Institution Order*, CUA provided a description of "local partners" and Resold Services, i.e., dark fibers, data center services, and system integration. CUA Response to *Institution Order* at 47. CUA asserts that none of these Resold Services "require a FCC authorization" and none of the services provided by CUA's local partners to CUA's end-users are telecommunications services provided pursuant to an FCC authorization. *Id*.

[37] CUA Response to *Institution Order* at 44-45.

[38] *See generally Order to Show Cause*, 35 FCC Rcd 3721; *see also id.*, 35 FCC Rcd at 3725-26, paras. 9, 11. In the *Order to Show Cause*, the Bureaus also asked CUA to explain why the Commission should not reclaim CUA's three International Signaling Point Codes (ISPCs). *Id*. On March 10, 2021, based on the information CUA filed in response to the *Order to Show Cause*, the International Bureau reclaimed the three ISPCs issued to CUA for failure to comply with the conditions of its provisional ISPC assignments after failing to notify the Commission of a transfer of an ISPC and is no longer using its three ISPC assignments. Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC, International Bureau, to Robert E. Stup, Jr. and Paul C. Besozzi, Counsel for China Unicom (Americas) Operations Limited, DA 21-227 (Mar. 10, 2021) (on file in GN Docket No. 20-110, File Nos. SPC-NEW-20030730-00031, SPC-NEW-20031009-00040, SPC-NEW-20070112-00002, ITC-

(continued….)

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.[39] In the *China Mobile USA 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.[40] 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 enterprise to the exploitation, influence, and control of the Chinese government.[41]

12. The Bureaus stated that such findings also raise questions as to CUA's ongoing qualifications to hold domestic and international section 214 authorizations, whether retention of these authorizations and ISPC assignments by CUA serves the public convenience and necessity, and whether its use of its ISPCs is consistent with the purpose for which they were assigned.[42] Accordingly, the *Order to Show Cause* directed CUA to respond to certain questions concerning its ownership, operations, and other related matters.[43] The Bureaus also directed CUA to explain "whether certain *pro forma* transfer of control actions occurred between 2009 and 2017 concerning the subject international section 214 authorizations and whether [CUA] appropriately notified the Commission, as required by Commission rules,"[44] and to provide "a description of the extent to which [CUA] is or is not otherwise subject to the exploitation, influence and control of the Chinese government."[45]

13. On June 1, 2020, CUA filed its response to the *Order to Show Cause*, including a public filing and a non-public business confidential filing.[46] CUA contends that the *Order to Show Cause* "provides no valid grounds for initiating a proceeding to revoke its long-standing section 214 authorizations to provide domestic and international services in the United States."[47] Among other arguments, CUA contends that (1) the main considerations under section 214 of the Act are competition

(Continued from previous page)
214-20020728-00361, ITC-214-20020724-00427 (ISPC Reclamation Letter). CUA did not file a response to the Bureau's letter.

[39] *Order to Show Cause*, 35 FCC Rcd at 3723-24, para. 5; *see China Mobile USA Order*, 34 FCC Rcd at 3361-62, 3380, paras. 1, 38.

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

[41] *Order to Show Cause*, 35 FCC Rcd at 3724, para. 6.

[42] *Id.* at 3724, para. 7.

[43] *Id.* at 3725-26, para. 9.

[44] *Id.* at 3726, para. 9; *see* 47 CFR §§ 63.18, 63.24(f).

[45] *Order to Show Cause*, 35 FCC Rcd at 3726, para. 9. The Bureaus also directed CUA to provide additional information regarding the services it provides and other information. *Id.* at 3725-26, para. 9. CUA's responses are incorporated in this Order.

[46] CUA Response to *Order to Show Cause*. On May 14, 2020, CUA filed a motion for an extension of the time for its response to the *Order to Show Cause*, requesting an additional 30 days to respond. China Unicom (Americas) Operations Limited, Motion for Extension of Time, GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427, at 1 (filed May 14, 2020) (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427). On May 19, 2020, the International Bureau's Telecommunications and Analysis Division granted CUA an extension of time to respond to June 1, 2020. Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Robert E. Stup, Jr., Counsel to China Unicom (Americas) Operations Limited, Squire Patton Boggs (US) LLP (May 19, 2020), 35 FCC Rcd 5334 (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427).

[47] CUA Response to *Order to Show Cause* at i.

in the market and protecting consumers from unnecessary costs, and not national security; (2) revocation of section 214 authority is a punitive sanction; (3) the partial and indirect ownership of CUA is not a sufficient basis to conclude that CUA presents a national security risk; (4) there are alternatives to revocation that have never been broached with CUA; and (5) revocation requires a full hearing.[48]

14. On October 15, 2020, the International Bureau issued a letter requesting that DOJ, on behalf of the Attorney General as Chair of the Committee under Executive Order 13913, address the arguments made by CUA in its response to the *Order to Show Cause*.[49] The letter sought "the Committee's views on [CUA's] arguments concerning whether and how it is 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 mitigation measures could address any identified concerns."[50]

15. On November 4, 2020, CUA filed a letter responding to the International Bureau's October 15, 2020 Letter to DOJ.[51] In its letter, CUA states that it remains committed to work in good faith to resolve the concerns raised in the *Order to Show Cause*.[52] CUA also argues that the International Bureau's request to the Committee for comment "is not consistent with either prior executive branch review practices or the new procedures just established by the Commission."[53] CUA "firmly believes that a thorough and fair Committee review could result in a mitigation agreement to address any national security or law enforcement concerns."[54] Among other arguments, CUA "renews its objection to any action by the Commission to revoke [CUA's] section 214 authorizations without providing [it] a hearing with all of the substantive and procedural rights afforded under the Commission's rules."[55]

16. On November 16, 2020, the National Telecommunications and Information Administration (NTIA), on behalf of the Executive Branch, responded to the International Bureau's October 15, 2020 Letter.[56] The Executive Branch agencies identify a number of national security and law

[48] *Id*. at i-ii, 2-16.

[49] 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 11488 (October 15, 2020 Letter) (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427).

[50] *Id.* at 11490.

[51] Letter from Robert E. Stup, Jr., Counsel to China Unicom (Americas) Operations Limited, Squire Patton Boggs (US) LLP, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau (Nov. 4, 2020) (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427) (Nov. 4, 2020 China Unicom Americas Letter to the FCC). On November 4, 2020, CUA also filed a letter with DOJ, requesting "(i) that the Committee request from the Commission additional time to respond to the Request and (ii) the opportunity to engage with the Committee to provide up-to-date information regarding its operations and to discuss possible mitigation measures necessary to address the national security and law enforcement concerns of the Committee." Letter from Robert E. Stup, Jr., Counsel to China Unicom (Americas) Operations Limited, Squire Patton Boggs (US) LLP, to Sanchitha Jayaram, Chief, Foreign Investment Review Section, National Security Division, U.S. Department of Justice (Nov. 4, 2020) (on file in GN Docket No. 20-110).

[52] Nov. 4, 2020 CUA Letter to the FCC at 2 (citing CUA Response to *Order to Show Cause* at 9).

[53] *Id.* at 3.

[54] *Id*. at 4.

[55] *Id*.

[56] 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 CUA" due to "the nature of the

(continued….)

enforcement concerns regarding CUA.[57] The Executive Branch agencies state that CUA "is subject to exploitation, influence, and control by the [Chinese] government"[58] and "changes in [Chinese] law have resulted in [Chinese]-owned and -controlled companies presenting significant national security and law enforcement risks that are difficult to mitigate."[59] The agencies state that "the same national security and law enforcement concerns the Executive Branch raised in the [China Telecom (Americas) Corporation (China Telecom Americas)] and [China Mobile USA] recommendations apply equally to" CUA.[60] The Executive Branch agencies add that the "lack of trust . . . renders CUA's recent submission to the [Commission] and recent outreach to DOJ regarding mitigation measures an illusory proposition."[61] The Executive Branch agencies note CUA's responses to Congress that were described in 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).[62]

17. On December 9, 2020, CUA filed a response to the Executive Branch Letter.[63] This response contends that the Executive Branch Letter does not recommend that the Commission take any

(Continued from previous page)
Commission's request for views on discreet [sic] factual questions, and the limited time allotted for response." *Id*. at 1.

[57] The Executive Branch agencies' concerns include: (1) changed circumstances in the U.S. national security environment, including the U.S. government's increased concern in recent years about malicious cyber activities undertaken at the direction of the Chinese government; (2) CUA's status as a wholly owned subsidiary of a Chinese state-owned enterprise that is ultimately owned and controlled by the Chinese government; (3) CUA's and its parent entities' commercial relationships with Chinese entities accused of engaging in malicious activities contrary to U.S. national security and economic interests; and (4) CUA's U.S. operations, which provide opportunities for increased Chinese state-sponsored cyber activities, including economic espionage, the disruption and misrouting of U.S. communications traffic, and access to U.S. records and other sensitive data. *See generally* Executive Branch Letter.

[58] *Id*. at 37.

[59] *Id*. at 2.

[60] *Id*. at 6 (citing Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate China Telecom Americas' International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 at 1 (filed Apr. 9, 2020) (Executive Branch CTA Recommendation) (filing with the Commission a public filing, a non-public business confidential filing, and a classified appendix); Redacted Executive Branch Recommendation 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)); *see also* Executive Branch CTA Recommendation at 1-7, 41-43 (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 opportunities for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic).

[61] Executive Branch Letter at 37 (citing Letter to Department of Justice from China Unicom Americas, In the Matter of China Unicom (Americas) Operations Limited, GN Docket No. 20-110; File Nos. ITC-214-20020728-00361; ITC-214-20020724-00427 (Nov. 4, 2020), https://go.usa.gov/xeFF7; Letter to Federal Communications Commission from China Unicom Americas, In the Matter of China Unicom (Americas) Operations Limited, GN Docket No. 20-110; File Nos. ITC-214-20020728-00361; ITC-214-20020724-00427 (Nov. 4, 2020), https://go.usa.gov/xeFFd).

[62] Executive Branch Letter at 1-17, 32, 35-36 (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://go.usa.gov/xeUZZ (PSI Report)).

[63] Letter from Robert E. Stup, Jr., Counsel to China Unicom (Americas) Operations Limited, Squire Patton Boggs (US) LLP, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau (Dec. 9, 2020) (on file in GN Docket No. 20-110, File Nos. ITC-214-20020728-00361, ITC-214-20020724-00427) (CUA Reply to Executive Branch Letter).

action against CUA, nor does the Executive Branch Letter "so much as hint at a single action of CUA that raises national security or law enforcement concerns or a single respect in which CUA has fallen short of its obligations under U.S. law."[64] In the absence of such allegations, CUA contends it "has nothing to which to respond."[65] CUA states that the Executive Branch Letter "offers a series of broad, policy-based views about how, in general, the FCC should consider Chinese government ownership in granting and revoking section 214 authorizations," and argues that the use of such policy rationales would be a departure from the Commission's longstanding rules and precedents and cannot be used as the basis for a revocation proceeding in the absence of any identifiable conduct warranting such an action.[66] In this regard, among other arguments, CUA contends that revoking a section 214 authorization based on general policy considerations would require notice-and-comment rulemaking.[67]

18. *Institution Order*. On March 17, 2021, we adopted the *Institution Order* to institute a proceeding to revoke the domestic authority and the international authorizations issued to CUA pursuant to section 214 of the Act.[68] We stated that CUA had failed at that stage to dispel serious concerns regarding its retention of section 214 authority in the United States.[69] Among other things, the *Institution Order* stated 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 [CUA] has not yet adequately demonstrated that it is not susceptible to the exploitation, influence, or control of the Chinese government."[70] The *Institution Order* also noted that CUA's "representations to the Commission and to other U.S. government agencies raise significant concerns regarding whether [CUA] should retain its domestic section 214 authority and international section 214 authorizations," and we found that CUA "omitted crucial information in this proceeding that was disclosed to the [U.S.] Senate Subcommittee and published in the PSI Report, and failed to fully respond to several questions posed by the *Order to Show Cause*."[71] The *Institution Order* also adopted procedures allowing CUA, interested Executive Branch agencies, and the public to present further arguments or evidence in this matter.[72]

19. *Comments*. In accordance with the procedures established in the *Institution Order*, on April 28, 2021, CUA submitted a filing responding to the questions in the *Institution Order* and provided responses as to why the Commission should not revoke its section 214 authority. The Commission did not receive any filings responding to CUA's April 28, 2021 filing, nor did CUA file any additional evidence or arguments.

III. DISCUSSION

20. After providing CUA several opportunities to respond with its own evidence and to make any factual or legal arguments contending otherwise, we find, based on our public interest analysis under section 214 of the Act and the totality of the substantial record evidence, that the present and future public

[64] *Id*. at 2.

[65] *Id*.

[66] *Id*.

[67] *Id*.

[68] 47 U.S.C. § 214; *see generally Institution Order*.

[69] *Institution Order*, 36 FCC Rcd at 6319-20, para. 1 (citing *China Telecom Americas Institution Order*, 35 FCC Rcd at 15006-07, paras. 1-2; *Order to Show Cause*, 35 FCC Rcd at 3724, para. 6; *China Mobile USA Order*, 34 FCC Rcd at 3363-64, 3365-66, 3369-70, paras. 3, 8, 17-18).

[70] *Institution Order*, 36 FCC Rcd at 6335, para. 26.

[71] *Id*. at 6353, para. 49.

[72] *Institution Order*, 36 FCC Rcd at 6320, 6359, 6360, paras. 1, 61, 66.

interest, convenience, and necessity is no longer served by CUA's retention of its section 214 authority. We first discuss the Commission's standard of review and how the procedures adopted in this proceeding comply with constitutional and statutory requirements and are consistent with Commission policy and precedent. We then discuss the substantial record evidence mandating that we revoke CUA's domestic section 214 authority and international section 214 authorizations, as well as our finding that mitigation will not address the significant national security and law enforcement concerns in this matter.

A. Standard of Review

1. Commission Authority

21. As a threshold matter, we find that the Commission has the authority to revoke a carrier's section 214 authority. CUA contends that the Commission "does not have the authority to revoke a section 214 authorization based on a change in policy."[73] CUA states that authorizations under the Act "are 'certificate[s] . . . [of] public convenience and necessity,' . . . ."[74] and that, pursuant to *Seatrain Lines, Inc.*, such certificates "when finally granted, and the timefixed for rehearing it has passed, [are] not subject to revocation in whole or in part except as specificallyauthorized by Congress."[75] CUA further contends that courts have applied this doctrine to certificates of public convenience and necessity and similar licenses under other statutes, such as the Interstate Commerce Act, the Mineral Leasing Act, citing to *Chapman v. El Paso Natural Gas Co.*, and the Federal Power Act, citing to *Hirschey v. FERC*.[76] CUA argues that "[l]ike those statutes, the Act says nothing about revoking a 'certificate' issued under section 214(a)," and that such "silence" is intentional[77] given the "multiple ways and circumstances [Congress prescribed] for suspending or revoking a spectrum license."[78]

22. We are not persuaded by CUA's arguments and find the *Seatrain*, *Chapman*, and *Hirschey* cases inapplicable with regard to the Commission's authority to revoke section 214 authorizations. In *Seatrain*, the Supreme Court noted that the agency itself had advised Congress that revocation authority was unnecessary, and that in other contexts the agency had viewed its revocation authority as limited.[79] In this case, in contrast, as noted herein, the Commission has repeatedly asserted its revocation authority over section 214 authorizations. In *Chapman*, the U.S. Court of Appeals for the D.C. Circuit concluded that regulating the operation of a gas pipeline was within "the plenary jurisdiction

---

[73] *See* CUA Response to *Institution Order* at 3-4. CUA contends that when "the Commission granted CUA its section 214 authorizations nearly twenty years ago[,] CUA's ultimate corporate parent was majority-owned by the Chinese government at the time, and [CUA] did not withhold or conceal that or any other relevant fact. The Commission made its decision to issue the authorizations after consideration of all the statutory and policy factors that the Commission deemed relevant at the time." *Id.* at 3. CUA adds that "now the Commission wants to revoke the authorizations because of general concerns that the Chinese government's ownership interest makes CUA's holding of section 214 authorizations a risk." *Id.*

[74] *Id.* at 3 (citing 47 U.S.C. § 214(a)).

[75] *Id*. (citing *United States v. Seatrain Lines, Inc.*, 329 U.S. 424, 432-33 (1947) (Interstate Commerce Act); *Chapman v. El Paso Natural Gas Co.*, 204 F.2d 46 (D.C. Cir. 1953) (Mineral Leasing Act); *Hirschey v. FERC*, 701 F.2d 215 (D.C. Cir. 1983) (Federal Power Act)).

[76] *Id*. (citing *Seatrain Lines, Inc.*, 329 U.S. at 432-33 (holding the Interstate Commerce Commission was "without authority to revoke" a common carrier's "certificate of public convenience and necessity")).

[77] *Id*. at 4 (citing *Nat'l Fed. of Indep. Businesses v. Sebelius*, 567 U.S. 519, 544 (2012) ("Where Congress uses certain language in one part of a statute and different language in another, it is generally presumed that Congress acts intentionally.")).

[78] *Id*. at 4 (citing 47 U.S.C. §§ 312(a), 303(m), 316). In sum, CUA states that "[w]hat the Commission proposes to do in this matter is something that Congress explicitly authorized for spectrum licenses and just as clearly did not allow for section 214(a) certificates." *Id.*

[79] *Seatrain Lines*, 329 U.S. at 430-31.

of the Federal Power Commission," not the Secretary of the Interior seeking to regulate such operations through a prior stipulation regulating the physical aspects of rights of way over federal lands.[80] The court further noted that "[i]t may well be appropriate for a licensing authority to reopen proceedings" based on "newly discovered or supervening facts,"[81] in contrast with the rationale for the Secretary's action. In *Hirschey*, whatever authority existed under the licensing requirements of the Federal Power Act, the U.S. Court of Appeals for the D.C. Circuit noted that vacating an exemption from those requirements would "make a sham" of "carefully crafted . . . regulations," governing such exemptions,[82] whereas here the Commission's exercise of revocation authority pursuant to the Communications Act is, as noted below, consistent with its prior views on that question. Further, as the Commission concluded in the *CCN, Inc. Order*, Section 4(i) also supports revocation authority, as reasonably ancillary to the Commission's authority to authorize common carrier service in the first instance.[83] Here, certainly no less so than as Congress recognized with respect to spectrum licenses,[84] such authority is necessary to ensure not only compliance with the Commission's rules and its requirements for truthfulness, but also that circumstances with serious national security and law enforcement consequences that would have been relevant in determining whether to authorize service remain relevant in light of significant developments since the time of such authorization.

23. Here, 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 . . . ."[85] When the Commission grants section 214 authority, it allows carriers to operate pursuant to a set of rules that include blanket section 214 authority in the domestic context[86] or on a global basis in the international context.[87]

24. With regard to revocation of a domestic section 214 authorization, as we explained above, 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.[88] 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

[80] *Chapman*, 204 F.2d at 52.

[81] *Id.* at 53-54.

[82] *Hirschey v. FERC*, 701 F.2d at 218.

[83] *CCN, Inc. Order*, 13 FCC Rcd at 13607.

[84] *See* 47 U.S.C. § 312(a) (revocation authority, *inter alia*, for false statements knowingly made, willful or repeated noncompliance with license terms, willful or repeated violation of the Act or Commission rules, or "conditions coming to the attention of the Commission which would warrant it in refusing to grant . . . an original application"). Indeed, section 214—unlike section 312—contains no limitation on the circumstances that might justify revocation. *See also* 49 U.S.C. § 312 (1946 ed.), cited in *Smith Bros. Revocation of Certificate*, 33 M.C.C. 465, 471-72 (1942) and discussed in *Seatrain*, 329 U.S. at 430-31, in which Congress specifically provided that motor carrier certificates "shall remain in effect until suspended or terminated as herein provided." To the same effect is the framework of the Federal Aviation Act. *See* 49 U.S.C. § 41110.

[85] 47 U.S.C. § 214(a).

[86] 47 CFR § 63.01.

[87] 47 CFR §§ 63.10 through 63.25.

[88] *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11365-66, para. 2. The Commission did not extend this blanket authority to international services. *Id.* at 11365-66, para. 2 & n.8; 47 CFR § 63.01.

to protect the public interest.[89] With regard to revocation of an international section 214 authorization, the Commission in the *Foreign Participation Order* and the *Reconsideration Order* 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.[90] In the *Foreign Participation Order*, the Commission also stated it considers "national security" and "foreign policy" concerns when granting authorizations under section 214 of the Act.[91] Indeed, promotion of national security is an integral part of the Commission's public interest responsibility, including its administration of section 214 of the Act,[92] and is one of the core purposes for which Congress created the Commission.[93] Given these established statutory directives and longstanding Commission determinations, the Commission has authority to revoke section 214 authority. As such, CUA was fully on notice when its international section 214 authorizations were granted in 2002 that the Commission had authority to revoke its section 214 authorizations and that its authorizations were subject to revocation based on the Commission's consideration of the public interest.[94] As we describe below, the national security environment with respect to China has changed since CUA was authorized to provide telecommunications services in the United States, supporting our decision to revoke CUA's section 214 authority.[95]

2. Applicable Standard of Proof

25. Consistent with applicable law, we use the preponderance of the evidence as the standard of proof in reviewing the full record to determine whether revocation of CUA's domestic section 214 authority and international section 214 authorizations is warranted.[96] CUA contends that "[t]he traditional standard of proof required in a civil or administrative proceeding is proof by a preponderance of the

---

[89] *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.

[90] *See, e.g.*, *Foreign Participation Order*, 12 FCC Rcd at 24023, para. 295; *Reconsideration Order*, 15 FCC Rcd at 18173, para. 28; *id*., 15 FCC Rcd at 18175-76, para. 35; *see also* 47 CFR § 63.11(g)(2); *ECO Test Report and Order*, 29 FCC Rcd at 4259, 4266, paras. 6, 22.

[91] *Foreign Participation Order*, 12 FCC Rcd at 23919-20, paras. 61-63 (in regulating foreign participation in the U.S. telecom market in the late 1990s, the Commission recommitted to considering "national security" and "foreign policy" concerns when granting licenses under section 310(b)(4) and authorizations under section 214(a) of the Act, stating it would also continue to "accord deference" to expert Executive Branch views on these issues that would inform its "public interest analysis").

[92] The Commission has long considered national security as part of its section 214 public interest analysis. *See Hawaiian Tel. Co. v. FCC,* 589 F.2d 647, 657 (D.C. Cir. 1978) (noting Commission's review of "considerations of national security" under public interest standard in adopting satellite policy); *Foreign Participation Order*, 12 FCC Rcd 23919-20, paras. 61-63; *China Mobile USA Order*, 34 FCC Rcd at 3372, 3376–77, paras. 7–11; *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10963-64, para. 9; *China Telecom Americas Institution Order*, 35 FCC Rcd 15006; *Institution Order*, 36 FCC Rcd 6319; *Pacific Networks Corp./ComNet Institution Order*, 36 FCC Rcd 6368; *Huawei Techs. USA, Inc. v. FCC*, 2 F.4th 421, 440 (5th Cir. 2021); *China Telecom Americas Order on Revocation and Termination* at *2, *6, paras. 5, 17.

[93] 47 U.S.C. § 151; *see Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66, *recon. denied*, *Reconsideration Order*, 15 FCC Rcd 18158; *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11436, para. 34, *aff'd. Huawei Technologies USA v. FCC,* 2 F.4th at 439.

[94] *See supra* para. 6.

[95] *See infra* para. 76.

[96] *Steadman v. SEC,* 450 U.S. 91, 101 & n.21 (1981) (citing *Sea Island Broadcasting Corp. of S.C. v. FCC,* 627 F.2d 240, 243 (D.C. Cir. 1980)); *James A. Kay, Jr.*, 17 FCC Rcd 1834, 1837, para. 11 (2002) (subsequent history omitted).

evidence."[97] Additionally, CUA contends that "[t]he preponderance standard must be applied unless the type of case and the sanctions or hardship imposed require a higher standard,"[98] and that "[t]he clear-and-convincing standard might apply 'where particularly important individual interests or rights are at stake.'"[99] It states that such interests or rights could include "the potential deprivation of individual liberty, citizenship, or parental rights."[100] Moreover, CUA suggests that "[t]he Commission has been held to the clear-and-convincing evidence standard in license revocation cases in the past, where the court held that this standard would not "'significantly burden' [the Commission's] efforts to regulate licensees in furtherance of the public interest."[101]

26. We are unpersuaded by CUA's arguments that the clear and convincing standard should apply in this case. As we stated in the *China Telecom Americas Order on Revocation and Termination*, we find that "in the absence of any statutory requirement to the contrary, the standard of proof governing administrative hearings is the well-established 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."[102] CUA's reliance on *Sea Island*—in which the D.C. Circuit held that revocation of a license to operate an AM radio station was governed, at the agency level, by the "clear and convincing" standard of proof, rather than the "preponderance of evidence" standard that the Commission had applied in that case—is misplaced.[103] Indeed, as we previously explained, only a year after the D.C. Circuit's opinion in *Sea Island*, the Supreme Court held in *Steadman* that the standard of proof for adjudicatory proceedings subject to the APA is the "preponderance of the evidence," thereby eliminating the rationale for the D.C. Circuit's opinion in *Sea Island*.[104] We therefore find, consistent with applicable law, that the appropriate standard of proof in this proceeding is the preponderance of the evidence standard.

3. Public Interest Standard

27. CUA asserts that "[r]evocation of section 214 authorizations is a major penalty, heretofore reserved for the most serious cases of repeated and willful violations of the Commission's rules"[105] and argues that "[t]he conclusory allegations set forth in the [*Institution Order*] do not establish the kind of egregious misconduct that the Commission previously has required to justify revocation of section 214 authorizations."[106] Although CUA acknowledges that the Commission has previously

---

[97] CUA Response to *Institution Order* at 17 (citing *Sea Island*, 627 F.2d at 243, *cert. denied*, 449 U.S. 101 S. Ct. 105 (1980); *Jones ex rel. Jones v. Chater*, 101 F.3d 509, 512 (7th Cir. 1996) ("The preponderance of the evidence is the proper standard, as it is the default standard in civil and administrative proceedings."); *Collins Securities Corp. v. SEC*, 562 F.2d 820, 823 (D.C. Cir. 1977); *Bender v. Clark*, 744 F.2d 1424, 1429 (10th Cir. 1984)).

[98] *Id.* (citing *Woodby v. Immigration & Naturalization Serv.,* 385 U.S. 276, 286 (1966); *Collins,* 562 F.2d at 823-826)).

[99] *Id.* (citing *Herman & Maclean v. Huddleston*, 459 U.S. 375, 389 (1983)).

[100] *Id.* (citing *CEW Props. v. United States DOJ*, 979 F.3d 1271, 1278 (10th Cir. 2020); *Bender v. Clark*, 744 F.2d at 1429-30).

[101] *Id.* (quoting *Sea Island*, 627 F.2d at 244).

[102] *China Telecom Americas Order on Revocation and Termination* at *5, para. 15; *see Institution Order*, 36 FCC Rcd at 6328, para. 15, n.57 (citing 5 U.S.C. §556(d); *Steadman v. SEC,* 450 U.S. at 101 & n.21 (citing *Sea Island*, 627 F.2d 240); *James A. Kay*, *Jr.*, 17 FCC Rcd at 1837, para. 11 (subsequent history omitted)).

[103] CUA Response to *Institution Order* at 17, n.81 (citing *Sea Island*, 627 F.2d at 244).

[104] *China Telecom Americas Order on Revocation and Termination* at *5, para. 15, n.60 (citing *Steadman,* 450 U.S. at 104).

[105] CUA Response to *Institution Order* at 1.

[106] *Id*. at i; *see id.* at 2, 20. CUA also states that "[t]he Commission has historically revoked section 214 authorizations due to misconduct." *Id.* at 25. CUA further notes that "[s]ection 214 . . . does not contain any

(continued….)

revoked section 214 authorizations, CUA posits that even if such revocations were proper, "they show at most that the Commission can revoke a section 214 authorization as a punitive sanction, not that the Commission can revoke an authorization simply because its policy preferences have changed."[107] CUA identifies several cases between 1997 and 2007 that CUA argues demonstrate that the Commission "has only initiated section 214 revocation proceedings for cause (*e.g.*, in response to severe misconduct or willful violations of relevant laws and the Commission's rules or policies)."[108]

28. We affirm the Commission's prior determination that it is unreasonable to conclude that egregious or severe misconduct could be the only justification for revocation as argued by CUA,[109] given the Commission's ongoing responsibility to evaluate all aspects of the public interest, including national security and law enforcement concerns. Indeed, while section 312 of the Act does not apply here, it permits revocation of Title III licenses and permits based on 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."[110] As we stated in the *China Telecom Americas Order on Revocation and Termination*, "[t]he same principle applies to determinations of the public convenience and necessity under section 214 of the Act where the Commission has reserved its 'authority to enforce our safeguards through . . . the revocation of authorizations'[111] and explained that it grants 'blanket' and 'global' authorizations with the understanding that they may be revoked."[112] We therefore find that

(Continued from previous page)
reference to revocation. The most analogous provision in the Act is Section 312, which applies to revocation of station licenses and construction permits. 47 U.S.C. § 312(a)." *Id*. at 25, n.113.

[107] *Id*. at 4. CUA states that in undertaking such revocations, the Commission did not contemplate whether it has authority to do so and no court has reviewed the question regarding Commission authority. *Id.*

[108] *Id.* at 7-8, n.33 (citing *CCN, Inc. Order*, 12 FCC Rcd at 8548 (order to show cause following slamming investigation of numerous customer complaints that revealed "a pervasive pattern of questionable business and marketing practices under the Commission's rules"); *Publix Network Corp.*, 17 FCC Rcd 11487, 11503 (2002) (order to show cause where common carrier "unlawfully obtained over six million dollars in payments from the TRS Fund by means of a scheme to create the appearance that they were operating a legitimate telecommunications relay service"); *NOS Comm'cns, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6952, 6954 (2003) (*NOS Order*) (order to show cause where carrier "may have willfully or repeated violated" the 1934 Act "by conducting a misleading marketing campaign" by "threaten[ing] their former customers withloss of service unless they agreed to retain [the carrier's] services"), *case terminated by consent,* FCC 03M-42 (2003); *Business Options, Inc.*, 18 FCC Rcd 6881, 6881-82 (2003) (order to show cause following allegations that entity engaged in misrepresentation in responses submitted to Commission during a slamming investigation), *case terminated by consent*, 19 FCC Rcd 2916 (2004); *Kintzel Order*, 22 FCC Rcd 17197 (commencing evidentiary hearing before an administrative law judge to revoke 214 authorization after carrier "apparently willfully and repeatedly violated multiple Commission rules and provisions of the Act" by failing to make payments required by a consent decree, unlawfully discontinuing service, and engaging in slamming or cramming); *case terminated by consent*, FCC 09M-52 (2009)).

[109] CUA Response to *Institution Order* at i, 2, 7-8, 20.

[110] 47 U.S.C. § 312(a)(2).

[111] *China Telecom Americas Order on Revocation and Termination* at *6, para. 17.

[112] *Id.* (citing *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11372-73, 11374, paras. 12-14, 16; *Personal Communications Industry Association's Broadband Personal Communications Services Alliance's Petition for Forbearance for Broadband Personal Communications Services*, Memorandum Opinion and Order, 13 FCC Rcd 16857, 16881, para. 48 (1998) ("[W]e find that it is necessary to continue to require that international services be provided only pursuant to an authorization that can be conditioned or revoked.")). Thus, we are unpersuaded by CUA's contention that "Section 312(a)(2)[, the most analogous provision to section 214,] implies that there must be some act or omission of the licensee that warrants revocation" and that "the provision for license revocation based on new conditions is not a grant of total discretion to the FCC to revoke properly issued authorizations as a result of circumstances outside the control of the licensee." CUA Response to *Institution Order* at 25, n.113.

revocation based upon an assessment of the public interest, convenience, and necessity under section 214 of the Act may be based on other public interest factors coming to the attention of the Commission, including factors that may not be under the carrier's control.[113]

4. CUA Had Sufficient Notice and Several Opportunities to Be Heard

29. We reject CUA's various procedural arguments and find that the procedures we followed are consistent with principles of due process and applicable law and provided CUA with sufficient notice and several opportunities to be heard. In particular, CUA argues that its section 214 authorizations are protected property interests that are entitled to due process[114] and that its foreign ownership structure does not diminish its entitlement to due process.[115] CUA also asserts that it is entitled to an evidentiary hearing as required by due process and consistent with the Commission's established precedent.[116] Finally, CUA contends that revocation of CUA's section 214 authorizations because of a change in policy would be a taking.[117]

a. Procedures Satisfy Due Process Requirements

30. As an initial matter, we decline to address the merits of whether CUA's section 214 authorizations are protected property interests that are entitled to due process or the impact of its foreign ownership structure on its entitlement to due process. Rather, as we stated in the *Institution Order*, "[w]e 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."[118]

31. We reject CUA's contention that the Commission's decision not to designate this matter for an evidentiary hearing before an administrative law judge was arbitrary and capricious because the Commission would be violating the Due Process Clause and deviating from its own precedent. CUA contends that the Due Process Clause requires "the Commission give CUA the opportunity to present witnesses before an [administrative law judge]" and that "[n]otice and the opportunity to be heard 'must

---

[113] *See China Telecom Americas Order on Revocation and Termination* at *6, para. 17.

[114] CUA Response to *Institution Order* at ii, 4-9. CUA contends that "[c]ourts regularly recognize protected property interests in government-issued business licenses." *Id.* at 5 (citing *Barry v. Barchi*, 443 U.S. 55, 64 (1979); *Pro's Sports v. City of Country*, 589 F.3d 865, 872–73 (7th Cir. 2009); *Spinelli v. City of New York*, 579 F.3d 160, 169 (2d Cir. 2009); *Alaska Airlines, Inc. v. Civil Aeronautics Bd.*, 545 F.2d 194 (D.C. Cir. 1976)). Among other things, CUA argues that "[a] licensee is entitled to due process in a revocation action where it can show "more than a unilateral expectation" of the license's continuing effect. *Id.* (citing *3883 Conn. LLC v. Dist. of Columbia*, 336 F.3d at 1072). It asserts that, "[f]or a license to lack that status, the agency's discretion to take the license away must be 'significant' or 'unfettered'; when statutes or rules place some limit on that discretion (by, for example, imposing conditions on revocation), a license is a property right." *Id*. at 5-6 (citing *Spinelli*, 579 F.3d at 169; *3883 Conn. LLC*, 336 F.3d at 1072). CUA also asserts that "a licensee is entitled to due process prior to revocation where, as here, the underlying licensure rules and regulations "engendered a clear expectation of continued enjoyment of a license absent proof of culpable conduct." *Id*. at 6 (quoting *Barry*, 443 U.S. at 64, n.11).

[115] *Id*. at ii, 8-9 (citing as support for the proposition that foreign-owned entities such as CUA are entitled to due process, *GSS Grp.*, 680 F.3d at 815; PSI Report at 16 (June 9, 2020); *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10927, para. 92 (2020)).

[116] *Id.* at ii, 9-17.

[117] *Id*. at 21-22.

[118] *Institution Order*, 36 FCC Rcd at 6331, para. 19, n.74. *See* CUA Response to *Institution Order* at 4 ("Even assuming the Commission can in some situations revoke a section 214 authorization, the authorization is a property right, protected by the Due Process Clause.").

be granted at a meaningful time and in a meaningful manner.'"[119] Thus, CUA argues, depriving CUA of an evidentiary hearing prior to the revocation of its section 214 authorizations would be a violation of CUA's due process rights.[120] CUA also contends that the Commission did not address the three-part test from *Mathews v. Eldridge*, "[t]o determine whether due process require[d] live testimony" in this case, or whether "CUA's due process rights would be substantially protected."[121]

32. Contrary to CUA's claims, the Supreme Court has held that "the ordinary principle [is] that something less than an evidentiary hearing is sufficient prior to adverse administrative action."[122] The procedural requirements for formal adjudications under the APA[123] do not apply here,[124] and live evidentiary hearings are the rare exception rather than the norm. Courts have held that the question of whether to hold an evidentiary hearing is "within [the agency's] discretion, and it may 'properly deny an evidentiary hearing if the issues, even disputed issues, may be adequately resolved on the written record, at least where there is no issue of motive, intent or credibility.'"[125] That is the case here; we conclude that the ultimate decisions about revocation may be resolved on the present record. In fact, CUA has had several opportunities to respond to the Commission's concerns, beginning with the *Order to Show Cause*.[126] The *Institution Order*, in turn, provided CUA with a "further opportunity" to explain why "the *present and future* public interest, convenience, and necessity is served by its retention of its domestic and international section 214 authority and why the Commission should not revoke its domestic section 214 authority and international section 214 authorizations."[127]

33. We next consider the three factors of the *Mathews v. Eldridge* test: (1) "the private interest that will be affected by the official action;" (2) "the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards;" and (3) "the Government's interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail."[128] With regard to the first factor, CUA states that "CUA is a California corporation formed in 2002, with a significant history of operating in the United States and with more than 95% of its employees being local hires. . . . The determination of these serious and complex issues will have significant financial and operational ramifications for CUA (including the loss of its business and investments), its local

[119] CUA Response to *Institution Order* at 13 (citing *Fuentes v. Shevin*, 407 U.S. 67, 80-81 (1972) ("If the right to notice and a hearing is to serve its full purpose . . . it must be granted at a time when the deprivation can still be prevented.")).

[120] *Id*.

[121] *Id*. (quoting *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976)).

[122] *Mathews*, 424 U.S. at 343.

[123] *See* 5 U.S.C. §§ 554, 556, and 557.

[124] *See Procedural Streamlining of Administrative Hearings*, 35 FCC Rcd 10729, 10732, para. 9, n.24 (2020) (*Administrative Hearings Order*) (citing *United States v. Florida East Coast Railway Co.*, 410 U.S. 224, 234-38 (1973)); *Empresa Cubana Exportada de Alimentos y Productos Varios v. U.S. Dep't of Treasury*, 638 F.3d 794, 802 (D.C. Cir. 2011).

[125] *NRG Power Mktg., LLC v. FERC*, 718 F.3d 947, 959 (D.C. Cir. 2013) (quoting *Pac. Gas & Elec. Co. v. FERC*, 306 F.3d 1112, 1119 (D.C. Cir. 2002)). Even questions of intent do not necessarily require trial-type hearings, where no basis has been advanced for challenging a party's assertion as to its intent. *See Minisink Residents for Enlil. Pres. & Safety v. FERC*, 762 F.3d 97, 114-15 (D.C. Cir. 2014) (holding that FERC properly resolved an issue of intent on a written record).

[126] *Institution Order*, 36 FCC Rcd at 6331-32, para. 21; *see* CUA Response to *Order to Show Cause*; CUA Response to *Institution Order*.

[127] *Institution Order*, 36 FCC Rcd at 6328, para. 15.

[128] *Mathews*, 424 U.S. at 335.

workforce, and its U.S. customers."[129] While we recognize that revocation will have an impact on CUA and its customers, 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."[130]

34. With regard to the second *Mathews* factor, CUA has not shown the value of any additional process or how it would prevent erroneous deprivation. We find that the procedures the Commission followed satisfy the bedrock requirements of due process—notice and the opportunity to be heard "at a meaningful time and in a meaningful manner."[131] CUA contends that "[a] hearing is necessary in this case because there is an abundance of material facts that remain in dispute that should be examined in a hearing, as well as number of substantive and complex issues that can only be properly resolved in a hearing."[132] As discussed below, we are not persuaded by CUA's contention,[133] and CUA has not explained why the process the Commission afforded it, in which CUA submitted two full rounds of written comments to respond to the specific bases for revocation proposed in the *Order to Show Cause* and the *Institution Order*, does not provide it a meaningful opportunity to present its case. We find that it is more than sufficient due process in this context to provide CUA with timely and adequate notice of the reasons for revocation; opportunity to respond with its own evidence and to make any factual, legal, or policy arguments; access to all of the evidence the Commission considers; a written order from the Commission providing its preliminary reasoning; and opportunity to respond to the Commission's preliminary findings.

35. The third *Mathews* factor—the fiscal and administrative burden on the Government—weighs heavily in favor of the Commission. Courts have recognized that hearings before an administrative law judge, with live testimony and cross examination, impose significant temporal and cost burdens on agencies.[134] The burden on the government would be especially heavy in this case, as a trial before an administrative law judge could require participation by officials from other agencies.[135] More importantly, given the national security issues at stake, any resulting unwarranted delay could be

---

[129] CUA Response to *Institution Order* at 12; CUA Response to *Institution Order*, Business Confidential Exh. 6 at 1 ("{

]}").

Material set off by double brackets {[ ]} is business-confidential information and is redacted from the public version of this document.

[130] 47 U.S.C. § 214(a). It is especially unlikely that a company owned and controlled by a foreign government can claim that its private interests weigh substantially against this statutory "public convenience and necessity" condition. Although foreign government control of a U.S. carrier in and of itself is not grounds for depriving it of an international section 214 application, the Commission has made clear that national security, law enforcement, and foreign policy considerations are considered independently of other factors and are not subject to the general presumption in favor of entry. *See Foreign Participation Order*, 12 FCC Rcd at 23920-21, para. 65; *China Mobile USA Order*, 34 FCC Rcd at 3371-72, para. 20 & n.63.

[131] *See, e.g., Mathews*, 424 U.S. at 333 (citing *Armstrong v. Manzo*, 380 U.S. 545, 552 (1965)); *cf.* 5 U.S.C. § 558(c)(1)-(2) (permitting "revocation . . . of a license" following "notice by the agency in writing" of any basis for revocation and an "opportunity to demonstrate compliance").

[132] CUA Response to *Institution Order* at ii; *see id*. at 9-11. CUA further contends that "[a]dditional procedures to address . . . complex issues with significant ramifications would . . . provide additional benefit to CUA and an evidentiary hearing is essential to reaching a fair decision in this matter." *Id.* at 12.

[133] *See infra* paras. 42-43.

[134] *See, e.g., Chemical Waste Mgmt. v. U.S. EPA,* 873 F.2d 1477, 1485 (D.C. Cir. 1989); *G.E. v. EPA*, 595 F. Supp. 2d 8, 38-39 (D.D.C. 2009).

[135] *Mathews*, 424 U.S. at 347-49.

harmful.[136] As such, we are not persuaded by CUA's contentions that "[a]ny concern that there would be harm resulting from a delay due to holding an evidentiary hearing can likewise not be supported," and that "[i]f time is of the essence, the appropriate solution is not to bypass anevidentiary hearing in its entirety, but rather 'to structure an expedited hearing.'"[137] Again, CUA has given us no reason here to believe that live testimony would shed meaningful light on material facts. Thus, our *Mathews* analysis supports our conclusion that no live evidentiary hearing is required and that the process afforded to CUA here has been sufficient. Even if CUA has some cognizable private interest here, any such interest is substantially outweighed by the extensive process that we have followed, our conclusion that there would be little or no benefit from receiving live witness testimony, and the fiscal, administrative, and national security interests that would be harmed by further delay.

36. Furthermore, the procedures in this case address CUA's concerns that "the record already presents important factual disputes, requiring testimony and the testing of witnesses in a genuine hearing before a neutral adjudicator like an [administrative law judge]"[138] and that "[t]he facts, such as they are, . . . are clearly at a minimum unsettled and due process dictates that a hearing be held before an objective third party before CUA is stripped of its section 214 authorizations."[139] Even under the subpart B hearing rules that CUA would have the Commission apply, a hearing may be presided over by "an administrative law judge," "one or more commissioners," or "the Commission" itself.[140] Moreover, if the Commission were to delegate initial responsibility to an administrative law judge, 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 determinations.[141] In any event, CUA has not explained why the extra step of appointing an administrative law judge to preside prior to the Commission's independent review, rather than simply proceeding directly before the Commission, is necessary for or would enhance the ability of the Commission, which will be the ultimate arbiter, to decide any matter here. At no point in this proceeding has CUA been denied an opportunity to introduce evidence or arguments on its behalf, and the Commission's decision here is based on the entire record.[142]

b. Procedures are Consistent with the Commission's Rules, Past Practice, and Precedent

37. CUA argues that although the Commission's rules "do not specifically reference the procedures for revocation of section 214 authorizations, the Commission has, for over twenty years, applied the procedures regarding the revocation of a station license or a construction permit in section

---

[136] *See, e.g., California ex rel. Lockyer v. FERC*, 329 F.3d 700, 711, 713 (9th Cir. 2003) (agency has a strong interest in reaching a decision at the earliest practicable time when delay could endanger the agency's administrative mission by preventing it from acting to mitigate harm).

[137] CUA Response to *Institution Order* at 12 (citing *Marine Space Enclosures, Inc. v. Fed. Mar. Com.*, 420 F.2d at 588).

[138] *Id*. at 9.

[139] *Id*. at 48.

[140] 47 CFR § 1.241(a); *cf*. 5 U.S.C. § 556(b) (stating that a 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).

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

[142] With regard to the need for a neutral adjudicator or objective third party, CUA fails to argue with specificity why the Commission or any individual Commissioner would not be able to serve as a neutral or objective decisionmaker in this case—and it has never moved for the recusal of any Commissioner. Absent 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, we find this contention unpersuasive. *See, e.g.*, CUA Response to *Institution Order* at ii, 9, 48.

1.91 of the Commission's rules, to the revocation of section 214 authorizations by affording parties notice, an opportunity to respond, and a hearing before an [administrative law judge]."[143] CUA further contends that "[t]he Commission makes no attempt to justify a deviation from this established practice, other than to state that it has authority to conduct its section 214 revocation proceedings as it chooses."[144] We disagree. The procedures adopted and outlined in the *Institution Order* are consistent with the Commission's rules, past practice, and precedent and are sufficient to resolve the ultimate questions in most section 214 cases while providing carriers with due process.[145] Specifically, we reject CUA's argument that "[u]ntil now, the Commission has consistently interpreted its own rules as requiring that issues in revocation proceedings be designated for hearing."[146]

38. As explained in the *Institution Order* and in similar cases,[147] 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"[148] includes the authority "to select the personnel and procedures that are best suited to the issues raised in each case and that will achieve a full, fair, and efficient resolution of each hearing proceeding."[149] While the Commission has relied upon live formal hearings before an administrative law judge where the Act requires designation of a matter for hearing under section 309 of the Act,[150] it has used other procedures for different types of proceedings when

[143] *Id*, at 13.

[144] *Id*. at ii; *see id*. at 15-16.

[145] We reject again CUA's arguments that (1) the Commission cannot proceed with revocation of CUA's section 214 authority absent a formal recommendation from the Committee; (2) the Commission did not provide the Executive Branch agencies sufficient time to properly evaluate its response and analyze the relevant national security considerations, given the "limited allotted time for response"; and (3) CUA was not afforded the opportunity to engage the Committee regarding mitigation. *See* CUA Response to Executive Branch Letter at 3-6; CUA Response to *Institution Order* at iii, 30-31. The Executive Branch agencies specifically state that their response is not offered as a recommendation by the Committee pursuant to Section 6 of Executive Order 13913. Instead they have offered their views pursuant to their discretion to communicate information to the Commission under the Executive Order. Executive Branch Letter at 1 (citing, for example, Executive Order 13913, §§ 10(h)(ii), 12(a)(i)). The Commission does not require a formal "recommendation" from the Committee but can consider the information provided by the relevant Executive Branch agencies in making its public interest determination. Additionally, the Executive Branch agencies have advised that mitigation measures will likely not address their significant national security and law enforcement concerns. *Id*. at 37-38. The Executive Branch agencies further state that CUA's offers to engage in discussions regarding mitigation measures "cannot resolve the national security and law enforcement concerns that result from its relationship to the [Chinese Communist Party] and [Chinese] government." *Id*. at 37; *see infra* Section C.

[146] CUA Response to *Institution Order* at ii; *see id*. at 13-15. As explained herein, we similarly reject CUA's contention that "[t]he Commission has previously afforded targets of potential section 214 revocations the opportunity to respond to allegations in an evidentiary hearing before an objective Administrative Law Judge." *Id*. at ii; *see id*. at 4.

[147] *Institution Order*, 36 FCC Rcd at 6328-29, para. 16; *China Telecom Americas Institution Order*, 35 FCC Rcd at 15015, para. 16; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6377-78, para. 14; *China Telecom Americas Order on Revocation and Termination* at *7, para. 20.

[148] 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" by section 4(j) of the Act, "so long, of course, as it observes the basic requirements designed for the protection of private as well as public interest"); *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").

[149] *Administrative Hearings Order*, 35 FCC Rcd at 10731, para. 7.

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

appropriate. 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.[151] Even when section 309 of the Act applies, the Commission has at times found it appropriate to proceed on the written record, for example, 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.[152] In fact, in the 2020 *Administrative Hearings Order*, the Commission adopted new rules and updated existing rules, including to part 1, subpart B (subpart B hearing rules), governing administrative hearings under the Act to "expand the use of a process that relies on written testimony and documentary evidence in lieu of live testimony and cross-examination."[153]

39. As we previously observed,[154] there is no statutory obligation that requires us to follow any specific procedures in the instant matter.[155] CUA identifies several cases between 1997 and 2009 in which the Commission designated for hearing the revocation of section 214 authorizations.[156] Those cases, however, reflect nothing more than the Commission's lawful exercise of its discretion to order a hearing in a particular dispute under section 214 of the Act.[157] CUA previously acknowledged[158] that "under limited circumstances not applicable here, the Commission has terminated section 214 authorizations without an evidentiary hearing,"[159] but it asserts that "these cases involved licensees that had gone out of business and did not respond to notices from the Commission, or that had repeated and

---

[151] *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) (*South Dakota Order*) and 47 CFR §§ 1.720-.736).

[152] *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) (*T-Mobile Order*). CUA argues that our reliance on the *South Dakota Order* and the *T-Mobile Order* is misplaced. CUA Response to *Institution Order* at 16. *See Institution Order*, 36 FCC Rcd at 6328-29, para.16. We disagree. We find that we correctly cited to the *South Dakota Order* as an example of a section 204 tariff proceeding where the "Commission has . . . resolved issues on a written record and without an administrative law judge." *See id*. at 6328-29, para. 16. Similarly, we correctly cited to the *T-Mobile Order* for the proposition that "the Commission has found it appropriate to proceed on the written record, as . . . transfer proceedings where the Commission has determined that there are no substantial issues of material fact or credibility issues." *See id*.

[153] *Administrative Hearings Order* at 10729, para. 2; *see* 47 CFR §§ 1.201-.377 (rules governing hearing proceedings).

[154] *See China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *Institution Order*, 36 FCC Rcd at 6328-29, para. 16; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6377-78, para. 14.

[155] Additionally, as discussed below, the basis for instituting these proceedings does not turn on any disputed facts that would benefit from being examined in a hearing before an administrative law judge. *See infra* paras. 42-43.

[156] CUA Response to *Institution Order* at 13-15 (citing *CCN, Inc. Order to Show Cause*, 12 FCC Rcd 8547; *Publix Network Corp.*, 17 FCC Rcd 11487; *Business Options, Inc.*, 18 FCC Rcd 6881, *case terminated by consent*, 19 FCC Rcd 2916 (2004); *NOS Order*, 18 FCC Rcd 6952, *case terminated by consent,* FCC 03M-42 (2003); and *Kintzel Order*, 22 FCC Rcd at 17197, para. 1, *case terminated by consent*, FCC 09M-52 (2009)). Significantly, none of those matters were ultimately resolved through a hearing under the subpart B rules.

[157] *See China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *Institution Order*, 36 FCC Rcd at 6330, para. 18; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6379, para. 16; *Application of Oklahoma W. Tel. Co.*, Order, 10 FCC Rcd 2243, 2243-44, para. 6 (1995) (*Oklahoma W. Tel. Co. Order*) (stating that "the Commission has the discretion to designate for evidentiary hearing issues raised in the context of a Section 214 application").

[158] *See* CUA Response to *Order to Show Cause* at 12-13.

[159] CUA Response to *Institution Order* at 17.

uncured violations of certain security or law enforcement conditions placed on their licenses."[160] Although CUA attempts to distinguish those proceedings,[161] they demonstrate that the Commission has not applied subpart B hearing rules to all section 214 revocation proceedings. Thus, contrary to CUA's view, the Commission has never had an established practice of requiring subpart B hearings for all section 214 revocations.[162] Rather, we find that the handful of cases on which CUA seeks to selectively rely simply reflect the tailoring of procedures according to the circumstances of each case, and in the exercise of the Commission's broad procedural discretion under section 4(j) of the Act. Additionally, all of the cases CUA discusses predate the Commission's proceeding revising its subpart B hearing rules, in which the Commission explained that "'the hearing requirements applicable to Title III radio applications do not apply to Title II section 214 applications'" and that "hearing rights for common carriers under section 214 are comparatively limited."[163] The Commission added that it nevertheless has "discretion to designate for [Subpart B] hearing issues raised in a Section 214 application" on a case-by-case basis.[164]

40. We further disagree with CUA's contention that "[t]o depart from these precedents, the Commission must, at a minimum, 'display awareness that it is changing position and show that there are good reasons for the new policy'"[165] and that "[t]he Commission has not displayed that awareness so far; the [*Institution Order*] denies it even has an established precedent regarding the procedure for revoking a section 214 authorization. Nor does the Commission offer any serious justification for using a different procedure here."[166] As we stated in the *China Telecom Americas Order on Revocation and Termination*, the *Institution Order*, and the *Pacific Networks/ComNet Institution Order*, 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

---

[160] *Id*. (citing *Wypoint Telecom, Inc. Termination of Int'l Section 214 Authorization*, Order, 30 FCC Rcd 13431, para. 4 (IB-PD 2015) (*Wypoint Telecom Order*); *LDC Telecommunications, Inc.*, Revocation Order, 31 FCC Rcd 11661, 11662, para. 5 (EB-TCD, IB-TAD & WCB-CPD 2016) (*LDC Telecommunications Order*); *WX Communications Ltd. Termination of Int'l Section 214 Authorization*, Order, 34 FCC Rcd 1028, para. 5 (IB-TAD 2019) (*WX Communications Order*). The *Wypoint Telecom Order* and *WX Communications Order* addressed the termination (as opposed to revocation) of those carriers' respective international section 214 authorizations for failure to meet a condition of their authorizations, among other reasons. *See generally Wypoint Telecom Order*; *WX Communications Order*. The *LDC Telecommunications Order* revoked the carrier's domestic section 214 authority and international section 214 authorization for failure to pay regulatory fees after the carrier failed to respond to an order to show cause. *See generally LDC Telecommunications Order*.

[161] CUA contends that unlike these cases, "CUA currently provides telecommunications services to U.S. customers and has operated in compliance with its authorization conditions and obligations." CUA Response to *Institution Order* at 17.

[162] *China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *Institution Order*, 36 FCC Rcd at 6330, para. 18; *see also Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6379, para. 16.

[163] *Procedural Streamlining of Administrative Hearings*, Notice of Proposed Rulemaking, 34 FCC Rcd 8341, 8343, para. 4 & n.16 (2019) (*Administrative Hearings NPRM*). In the *Administrative Hearings Order*, the Commission adopted and incorporated by reference all the rules described in the *Administrative Hearings NPRM* with minor modification and adopted and incorporated by reference and further elaborated the legal arguments and justification presented in the *Administrative Hearings NPRM* in support of the rules adopted in the Order. *Administrative Hearings Order*, 35 FCC Rcd at 10731, para. 8.

[164] *Administrative Hearings NPRM*, 34 FCC Rcd at 8343, n.16 (citing *Oklahoma W. Tel. Co. Order*, 10 FCC Rcd at 2243-44, para. 6).

[165] CUA Response to *Institution Order* at 15 (citing *Jimenez-Cedillo v. Sessions*, 885 F.3d 292, 298 (4th Cir. 2018) (quoting *Encino Motorcars*, 136 S. Ct. at 2126). Failure to explain the reversal of directly controlling precedent is unlawful. *RKO Gen. v. FCC*, 670 F.2d 215, 223-24 (D.C. Cir. 1981); *Columbia Broadcasting System, Inc. v. FCC*, 454 F.2d 1018, 1026 (D.C. Cir. 1971); *Melody Music, Inc. v. FCC,* 345 F.2d730, 732 (D.C. Cir. 1965)).

[166] CUA Response to *Institution Order* at 15.

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.[167]

41. More importantly, the Commission has never applied its subpart B hearing rules to every adjudication.[168] Section 1.91 of the Commission's rules applies subpart B hearing rules to revocations of "station license[s]" or "construction permit[s]"—terms that refer to spectrum licenses issued under Title III of the Act—but, in contrast to an adjacent section of those rules, does not extend to section 214 authorizations.[169] This distinction reflects one in the Act itself, which specifies a procedure for revoking Title III authorizations in section 312,[170] but does not specify any such required procedure for revoking Title II authorizations. Thus, in the recent proceeding updating the Commission's subpart B hearing rules, the Commission noted that "the hearing requirements applicable to Title III radio applications do not apply to Title II section 214 applications."[171]

c. No Material Facts in Dispute Warranting a Hearing

42. Based on the record as a whole, we find that there are no substantial and material questions of fact in this matter warranting an adjudicatory hearing before an administrative law judge or other presiding officer.[172] The record available to the Commission when it issued the *Institution Order* supported such a preliminary view, and the current record developed since then has not persuaded us

---

[167] *China Telecom Americas Order on Revocation and Termination* at *8, para. 21; *Institution Order*, 36 FCC Rcd at 6330-31, para. 19; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6379-80, para. 17. Thus, we reject CUA's argument that because the Commission has cited section 1.91 of the rules in orders designating proposed revocation of section 214 authorizations for hearing, they are applicable in the instant case. CUA Response to *Institution Order* at 13-16. *See FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009); *see, e.g.*, *CBS Corp. v. FCC*, 785 F.3d 699, 708 (D.C. Cir. 2015).

[168] *See Administrative Hearings NPRM*, 34 FCC Rcd at 8343, para. 4 & n.16. 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.* at note 1.

[169] 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.").

[170] 47 U.S.C. § 312(c).

[171] *See Administrative Hearings NPRM*, 34 FCC Rcd at 8343, para. 4 & n.16 (internal quotations and alteration omitted); *Oklahoma W. Tel. Co. Order*, 10 FCC Rcd at 2243-44, para. 6 (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)). *See Institution Order*, 36 FCC Rcd at 6330, para. 17; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6379, para. 15.

[172] *Institution Order*, 36 FCC Rcd at 6331, para. 21. CUA argues that the existence of material factual issues generally requires an agency to conduct evidentiary hearing. CUA Response to *Institution Order* at 11 (citing *Air Line Pilots Association, International v. CAB*, 475 F .2d 900, 904 (1973); *Marine Space Enclosures, Inc. v. FMC*, 420 F. 2d 577, 589, n.36 (1969); *SEC v. Frank*, 388 F.2d 486, 491-492 (2nd Cir. 1968); *American Airlines, Inc. v. CAB*, 359 F. 2d 624, 633 (D.C. Cir. 1966)).

otherwise. CUA argues that it is entitled to a hearing because "the record already presents important factual disputes, requiring testimony and the testing of witnesses in a genuine hearing before a neutral adjudicator like an ALJ."[173] CUA notes that "for complex issues like those presented here, a hearing is particularly appropriate because disposition by other means 'creates a greater likelihood of administrative error, and invites a more skeptical judicial scrutiny'"[174] and thus "[t]here is . . . value in establishing a full-scale administrative record that might dispel 'any doubts about the true nature of [an agency's] action.'"[175] We disagree and, based on our review of the record, we confirm our preliminary assessment in the *Institution Order* that "the question of whether revocation is appropriate will [not] turn on disputed issues of fact, nor will the credibility of any material evidence in the record be reasonably questioned."[176] Rather, we conclude that this decision is supported by a preponderance of the overall record, including but not limited to facts that are not reasonably disputed as well as the assessments of the Executive Branch of the overall national security and law enforcement risks. The disputes here, as we observed in the *Institution Order*, "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 [CUA's] ultimate ownership and control by the Chinese government."[177]

43. We are also not persuaded by CUA's argument that "[e]ven if some facts are undisputed, the Commission cannot escape the need for a hearing by pretending it can decide this case solely on the basis of those facts, and dismissing all other factual disputes as 'immaterial' to its decision"[178] and that "[t]he issue of whether these undisputed facts are sufficient by themselves to justify revocation of section 214 authorizations is itself a material issue that must be designated for hearing."[179] Again, the matters

---

[173] CUA Response to *Institution Order* at 9.

[174] *Id*. at 11 (citing *Nat'l Air Carrier Ass'n v. Civil Aeronautics Bd*., 436 F.2d 185, 195 (D.C. Cir. 1970)).

[175] *Id*. at 11-12 (citing *ATX, Inc. v. United States Dep't of Transp.*, 41 F.3d 1522, 1528 (D.C. Cir. 1994)).

[176] *Institution Order*, 36 FCC Rcd at 6328-29, para. 16.

[177] *Id*. at 6331-32, para. 21. We therefore find unnecessary CUA's offer to present "witnesses to testify that CUA is not subject to or susceptible to Chinese government exploitation, influence, or control" or "testimony that it operates independently and without interference or control from its parent company, much less from the Chinese government that owns entities several steps up in the hierarchy above its immediate parent company." CUA Response to *Institution Order* at 10.

[178] CUA Response to *Institution Order* at 11.

[179] *Id*. CUA contends that that was "the Commission's approach taken in every prior contested section 214 revocation, where the issues designated for hearing included not only the finding of evidentiary facts, but also the question of whether the facts found justified revocation." *Id.* We disagree with this characterization. *See supra* paras. 39-41. We are also not persuaded that *United States v. Storer Broadcasting Co.*, 351 U.S. 192 (1956) and *Air North America v. Dep't of Transp.*, 937 F.2d 1427, 1430 (9th Cir. 1991) support CUA's argument that a hearing is warranted because, among other things, our actions represent "a particularized determination that necessarily involves an analysis of the facts that apply only to CUA and not to all holders of section 214 authorizations." CUA Response to *Institution Order* at 11 & n.50. In *Storer*, the Supreme Court held that the "full hearing" required under section 309 of the Act "means that every party shall have the right to present his case or defense by oral *or documentary evidence*, to submit rebuttal evidence, and to conduct such cross-examination *as may be required for a full and true disclosure of the facts*." *Storer*, 351 U.S. at 202 (italics supplied). Indeed, *Storer* upheld the ability of the Commission to dispense with individualized hearings where it had prescribed generally applicable rules to address the multiple ownership of broadcast stations. In *Air North America*, the Ninth Circuit upheld the Department of Transportation's decision to revoke, without a hearing, the airline's certificate of authority to provide air transportation for violating the agency's dormancy rule, notwithstanding the statutory requirement for notice and a hearing before revocation. *Air North America*, 937 F.2d at 1433-34. As we have discussed at length, CUA had several opportunities to present its case by documentary evidence to ensure the full and true disclosure of the facts, and, in any event, has not persuaded us that a full hearing before an administrative law judge is warranted in this

(continued….)

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 CUA's ultimate ownership and control by the Chinese government. And CUA has offered no new evidence that would dispel the Commission's prior analysis in the *Institution Order*, as discussed in detail below.[180] Finally, we find that the Commission is exercising its well-established discretion[181] to proceed without holding an evidentiary hearing, and we base our decision today on the overall assessment of the public interest.

d. Revocation of CUA's Section 214 Authority Is Not a Taking

44. Contrary to CUA's contention that revocation of its section 214 authority "amounts to a taking,"[182] we find that revoking CUA's section 214 authorizations does not implicate the Fifth Amendment's prohibition against the taking of private property "for public use, without just compensation."[183] Specifically, we find that CUA's section 214 authorizations are not private property for purposes of the takings clause. Moreover, even if CUA's section 214 authorization are a property interest, we find that our action herein does not amount to a taking, and we have provided CUA more than sufficient due process such that we can revoke its authorization consistent with the requirements of the Due Process Clause of the Fifth Amendment.

45. CUA contends that "FCC authorizations have been recognized as property that could be subject to a taking"[184] and that "[t]he Communications Act itself seems to imply the existence of a limited property right in an FCC authorization once it is granted."[185] CUA further asserts that Commission grant of a section 214 authorization "creates a highly valuable property right, in the development of which CUA, like other holders of section 214 authorizations, has made large investments of capital."[186] CUA also argues that "the seizure of the authorizations would anyway be far in excess of any [enforcement action] penalty that would be rational for the supposed misconduct that the Commission has identified."[187] CUA adds that revocation of CUA's section 214 authority based upon "a change in the Commission's foreign policy that is out of CUA's control and is not mentioned as a condition in CUA's original authorization application constitutes a taking[,]" and therefore "[t]he Commission must, in its decision making, take account of the cost it is undertaking, on behalf of the United States, to compensate CUA for this taking."[188]

46. We disagree with CUA's assertion that its section 214 authorizations are property that could be subject to a taking. Like spectrum licenses, section 214 authorizations do not create property

(Continued from previous page)
case. Thus, CUA's argument that "the issues posed in those cases were very different from those here, and their holdings are inapplicable to this proceeding," has no merit. CUA Response to *Institution Order* at 11, n.50.

[180] *See infra* Sections III.B-D.

[181] *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.").

[182] CUA Response to *Institution Order* at 21-22.

[183] U.S. CONST. amend. V.

[184] CUA Response to *Institution Order* at 22 (citing *Alpine PCS, Inc. v. United States*, 128 Fed. Cl. 303, 308 (Fed. Cl. 2016).)

[185] *Id*. at 22 (citing *IRS v. Subranni (In re Atl. Bus. & Cmty. Dev. Corp.)*, 994 F.2d 1069, 1073-74 (3d Cir. 1993)).

[186] *Id*. (citing *Yankee Network, Inc. v. FCC,* 107 F.2d 212, 217 (D.C. Cir. 1939)).

[187] *Id.* at 21 (citing *BMW of North America, Inc. v. Gore*, 517 U.S. 559).

[188] *Id*. at 22.

interests. Courts have generally affirmed that spectrum rights are not property rights subject to the Takings Clause[189] because they are, among other things, "limited by statute subject to the Commission's considerable regulatory power and authority."[190] Because the ability to obtain and retain section 214 authorizations is similarly limited by statute subject to the Commission's considerable regulatory power and authority, a section 214 authorization is analogous to a Title III spectrum license in this regard.[191]

47. Assuming *arguendo* that CUA's section 214 authority is a property interest, we believe our action—revoking CUA's section 214 authority due to significant national security and law enforcement concerns—does not amount to a taking under the *ad hoc* test set out in *Penn Central Transp. Co. v. New York City*.[192] Under the *Penn Central* test, the principal factors in determining whether a governmental regulation effects a taking are: (1) the character of the governmental action; (2) the economic impact of that action; and (3) the action's interference, if any, with investment-backed expectations.[193] The character of the governmental action, weighs heavily in favor of a finding that revocation of CUA's section 214 authority does not constitute a taking as "[c]ourts have been hesitant to find a fifth amendment taking where, as here, the government's alleged interference with property 'arises from a public program that adjusts the benefits and burdens of economic life to promote the common

[189] *Expanding Flexible Use of the 3.7 to 4.2 GHz Band*, Report and Order and Order of Proposed Modification, 35 FCC Rcd 2343, 2402, para. 145 (2020) (citing *NextWave Pers. Commc'ns, Inc.*, 200 F.3d 43, 51 (2d Cir. 1999), *cert. denied*, 531 U.S. 924 (2000) (citing 47 U.S.C. § 301 (the purpose of the Communications Act is to "to provide for the use of [radio] channels, but not the ownership thereof")); *FCC v. Sanders Bros. Radio Station*, 309 U.S. 470, 475 (1940) ("[N]o person is to have anything in the nature of a property right as a result of the granting of a license [under 47 U.S.C. § 301]"); *Celtronix Telemetry, Inc. v. FCC*, 272 F.3d 585, 589 (D.C. Cir. 2001) (noting that a license does not offer a vested right and that "it is undisputed that the Commission always retained the power to alter the term of existing licenses by rulemaking."); *Mobile Relay Associates v. FCC*, 457 F.3d 1, 12 (D.C. Cir. 2006) ("The Commission grants a licensee the right to 'the use of' the spectrum for a set period of time 'but not the ownership thereof."). *Cf. Alpine PCS, Inc. v. United States*, 128 Fed. Cl. 303, 309 (2016) (recognizing that a spectrum license can confer certain property rights that are limited by the terms, conditions and periods of the license but dismissing case on statute of limitations grounds), *aff'd*, 878 F.3d 1086, 1095-98 (Fed. Cir. 2018) (relying on different grounds to affirm lower court ruling that it lacked jurisdiction over appellant's regulatory takings claim, by holding that Communications Act displaced Tucker Act jurisdiction, and that the case fell within the exclusive jurisdiction of the D.C. Circuit under 47 U.S.C. § 403(b)(5)). We note that in affirming the lower court's rejection of the appellant's taking claim in *Alpine PCS*, the U.S. Court of Appeals for the Federal Circuit not only explained why jurisdiction for such a claim lay within the exclusive jurisdiction of the D.C. Circuit, but it also made it clear that it (the Federal Circuit) was accepting the appellant's premise that the spectrum licenses are "property protected by the Takings Clause . . . for purposes of assessing the jurisdictional issue" but "without deciding whether [such premise] is correct." *Alpine PCS*, 878 F.3d at 1095. *IRS v. Subranni*, which CUA relies on, did not hold that a broadcast license was "property" for purposes of a constitutional takings claim; rather, the question was whether, under the Internal Revenue Code, "proceeds from the sale of the license in a Chapter 7 bankruptcy proceeding are subject to [an Internal Revenue Service] lien." *IRS v. Subranni*, 994 F.2d at 1070, 1074-75.

[190] *Mobile Relay Associates*, 457 F.3d at 12; *see supra* paras. 4, 24, 28 (discussing the Commission's ability to condition and revoke section 214 authorizations). CUA's reliance on *Yankee Network, supra*, is misplaced. That decision predated the Supreme Court's unequivocal statement in *FCC v. Sanders Bros. Radio Station* that "[t]he policy of the [Communications Act] is clear that no person is to have anything in the nature of a property right as a result of the granting of a license." 309 U.S. at 475. *Accord*, *Mobile Relay Associates*, 457 F.3d at 11-12.

[191] *See Mobile Relay Associates*, 457 F.3d at 12. "The Commission grants a licensee the right to 'the use of' the spectrum for a set period of time 'but not the ownership thereof.'" *Id*. at 12 (citing 47 U.S.C. § 301)); *see also FCC v. Sanders Bros. Radio Station*, 309 U.S. at 475 ("The policy of the [Communications] Act is clear that no person is to have anything in the nature of a property right as a result of the granting of a license.").

[192] *Penn Central Transp. Co. v. New York City*, 438 U.S. 104 (1978) (establishing a test for determining whether governmental regulations result in a taking).

[193] *Id*. at 124.

good.'"[194] In this case, revoking CUA's section 214 authority clearly furthers the public interest, convenience, and necessity because it promotes a significant common good: ensuring national security and protecting the nation's communications infrastructure from potential security threats.[195]

48. CUA posits our action "will have significant financial and operational ramifications for CUA (including the loss of its business and investments), its local workforce, and its U.S. customers."[196] Even if that were the case, in the context of regulatory takings, "an investment-backed expectation must be reasonable," involving "an objective, but fact-specific inquiry into what, under all the circumstances, the [plaintiff] should have anticipated."[197] We find, based on the statutory imperatives and extant Commission policies at the time CUA obtained it section 214 authorizations, that CUA should have been aware that its 214 authorization was revocable in light of the Commission's regulatory regime and its expressed policies. Indeed, the Supreme Court has recognized, for example, with respect to property that "had long been subject to federal regulation," there was no "reasonable basis to expect" that the regulatory regime would not change.[198] Therefore, assuming CUA has a property interest in its section 214 authority, under the *Penn Central* test, we conclude that there has been no Fifth Amendment taking in this case that warrants just compensation. And in any event, as we have noted repeatedly, CUA has been provided more than sufficient due process, including notice of the Commission's significant concerns with CUA's retention of its section 214 authority as well as several opportunities to respond to the Commission's concerns.

B. Revocation of Section 214 Authority

49. Based on our public interest analysis under section 214 of the Act and the totality of the record evidence, we find that the present and future public interest, convenience, and necessity is no longer served by CUA's retention of its section 214 authority and therefore revoke CUA's domestic and international section 214 authority. *First*, the record shows that CUA, a U.S. subsidiary of a Chinese state-owned enterprise, is subject to exploitation, influence, and control by the Chinese government and is highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight. *Second,* given the changed national security environment with respect to China since the Commission authorized CUA to provide telecommunications services in the United States, we find that CUA's ties to the Chinese government—together with Chinese laws obligating CUA and its direct and indirect parent entities to cooperate with requests by the Chinese government—pose a clear and imminent threat to the security of the United States due to CUA's access to U.S. telecommunications infrastructure. *Third*, independent of these concerns, CUA's conduct and

---

[194] *Am. Cont'l Corp. v. United States*, 22 Cl. Ct. 692, 696 (Cl. Ct. 1991) (quoting *Connolly v. Pension Benefit Guar. Corp.*, 475 U.S. 211, 225 (1986)).

[195] In this regard, such action is a "valid regulatory measure[] taken to serve substantial national security interests" that courts have determined—in other contexts involving national security and foreign policy—is not a compensable taking for Fifth Amendment purposes. *See Paradissiotis v. United States*, 304 F.3d 1271, 1274-75 (Fed. Cir. 2002) ("[V]alid regulatory measures taken to serve substantial national security interests may adversely affect individual contract-based interests and expectations, but those effects have not been recognized as compensable takings for Fifth Amendment purposes."); *see, e.g.*, *767 Third Ave. Assocs. v. United States*, 48 F.3d 1575, 1581 (Fed. Cir. 1995). *See also Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation."); *Huawei Techs. USA, Inc. v. FCC,* 2 F.4th 421, 439–40 (5th Cir. 2021) ("[T]he FCC's considering national security under the public interest umbrella is not a new phenomenon.") (citing *Foreign Participation Order*, 12 FCC Rcd at 23919-20, paras. 61-63); 47 U.S.C. § 151 (protecting "national defense" is among the purposes of the FCC).

[196] CUA Response to *Institution Order* at 12.

[197] *A&D Auto Sales*, 748 F.3d at 1159 (quoting *Cienega Gardens v. U.S.*, 331 F.3d 1319, 1346 (Fed. Cir. 2003) (internal quotation marks omitted)).

[198] *Concrete Pipe & Prods.*, 508 U.S. 602, 645-46 (1993).

representations to the U.S. Congress and the Commission demonstrate a lack of candor, trustworthiness, and reliability that erodes the baseline level of trust that the Commission and other U.S. government agencies require of telecommunications carriers given the critical nature of the provision of telecommunications service in the United States.

1. The Chinese Government Indirectly Owns and Controls CUA

50. The record evidence overwhelmingly shows that CUA is not separate and independent from its parent entities[199] and supports the Executive Branch agencies' assessment that "CUA is indirectly majority-owned and -controlled by the [Chinese] government and therefore is vulnerable to exploitation, influence, and control by that government."[200] The record is clear that CUA "is indirectly and ultimately owned and controlled by the government of the People's Republic of China" through CUA's direct parent entity, CUG, and CUG's direct parent, CUHK, which are indirectly owned and controlled by CU, a Chinese state-owned enterprise.[201] The record also demonstrates that CUA and its parent entities are beholden to the Chinese government and the Chinese Communist Party. Further, contrary to CUA's contentions, we find that Chinese law—namely, the 2017 Cybersecurity Law, the 2017 National Intelligence Law, and the 2019 Cryptography law—requires CUA to support Chinese intelligence efforts.

51. In its response to the *Institution Order*, CUA argues that, "[a]s an independent corporation, CUA should be treated as sufficiently separate from the [Chinese] government."[202] CUA states that it "is governed in accordance with its Bylaws as well as its Articles of Incorporation," but that "review and approval by CUG is required for certain major corporate or business changes."[203] Further, CUA states that its "major decisions including internal reorganization, strategic plan, budget, investment etc., are first decided by CUA and then are subject to further approval by CUG."[204] CUA adds that "[t]hese requirements are all in accordance with California law, which allows for the requirement of shareholder approval 'for any corporate action.'"[205] Because CUG is CUA's sole shareholder, CUA states that "requiring its approval for certain decisions is not only completely lawful, but common among similarly structured corporations."[206] CUA contends that "[o]ther than CUG, no other entity that holds a ten percent or greater direct or indirect ownership interest in and/or controls CUA or has management and oversight of CUA's operations."[207]

---

[199] CUA Response to *Institution Order* at 36; *see also* CUA Response to *Order to Show Cause* at 9 ("CUA is a separate entity, headquartered in northern Virginia.").

[200] Executive Branch Letter at 20.

[201] *Institution Order*, 36 FCC Rcd at 6323, para. 5; *see* CUA Response to *Institution Order* at 31-33; CUA Response to *Order to Show Cause* at 16-18; *id*., Business Confidential Exh. 2; *Order to Show Cause*, 35 FCC Rcd at 3722-23, para. 4; *see supra* para. 7; *see infra* paras. 51-52. *See also* 2017 *Pro Forma* Notification, Attach. 1 at 2 (stating that "the [People's Republic of China] government continues to maintain ownership and control over CUA and will continue to do so.").

[202] CUA Response to *Institution Order* at 36; *see* CUA Response to *Order to Show Cause* at 9 (". . . CUA is a separate entity, headquartered in northern Virginia.").

[203] CUA Response to *Institution Order* at 33.

[204] *Id*. at 34.

[205] *Id*. (quoting Cal. Corp. Code § 204).

[206] *Id*. at 34-35.

[207] *Id*. at 35. We note that this statement by CUA reflects grammatical error. It appears that this grammatical error results, for example, from the inclusion of the word "that" (e.g., "[o]ther than CUG, no other entity that [sic] holds a ten percent or greater direct or indirect ownership interest in and/or controls CUA or has management and oversight of CUA's operations") or inclusion of the word "or" (e.g., "[o]ther than CUG, no other entity that holds a ten percent or greater direct or indirect ownership interest in and/or controls CUA or [sic] has management and oversight of CUA's operations").

52. CUA's argument that it is independent from its parent entities and the Chinese government is undermined by the record evidence. In a 2017 filing with the Commission, CUA stated that "the [People's Republic of China] government continues to maintain ownership and control over CUA and will continue to do so."[208] CUA has provided no evidence demonstrating that its ownership and control has changed since it made this statement in 2017. The record shows that CUG, as the sole shareholder of CUA, controls certain aspects of CUA's management, and that the Chinese government ultimately has influence and control over CUG. Contrary to CUA's claims, CUG does not simply provide input on "major decisions";[209] rather, CUG's control is much broader due to its role in CUA's decision making,[210] provision of services,[211] and access to and maintenance of U.S. customer records.[212] Moreover, CUA's assertion that it is "an independent corporation" that is "sufficiently separate from the [Chinese] government,"[213] is contradicted by the record evidence. As noted by the Executive Branch agencies, CUA's direct parent, CUG, "is a Hong Kong-registered entity, wholly owned by another Hong Kong entity, [CUHK]," which is ultimately "majority-owned and -controlled by the [Chinese] government" through its ownership by CU, a state-owned enterprise that is "under the direct supervision of [SASAC]."[214] The record evidence demonstrates that CUHK, as the sole shareholder of CUG, controls CUG and has the ability to influence and control CUA through CUG.[215] Further, as CUHK acknowledged in its filing with the U.S. Securities and Exchange Commission (SEC), CU is the "ultimate controlling shareholder" of CUHK.[216] CUA's failure to distinguish between voting and equity interest for each entity

[208] 2017 *Pro Forma* Notification, Attach. 1 at 2.

[209] CUA Response to *Institution Order* at 34. We reject CUA's argument that "CUG's ability to review and approve certain major decisions is no different than protections given to investors that the Commission has found do not convey 'control' over the regulated entity." *Id.* at 38 & n.140 (citing *Baker Creek Communications, LLC* [sic], Memorandum Opinion and Order, 13 FCC Rcd 18709, 18714-15, para. 9 (1998) and quoting from that Memorandum Opinion and Order, "'[p]ermissible investment protections typically give . . . a decision-making role, through supermajority or similar mechanisms, in major corporate decisions that fundamentally affect their interests'"). CUA omits the reference in the quoted statement to "minority shareholder." The Memorandum Opinion and Order stated, "[i]nvestment protection provisions, which are designed to protect *a minority shareholder's investment*, do not automatically constitute the potential to exercise control over an applicant. Permissible investment protections typically give *the minority shareholder* a decision-making role, through supermajority or similar mechanisms, in major corporate decisions that fundamentally affect their interests." *Application of Baker Creek Communications, L.P. For Authority to Construct and Operate Local Multipoint Distribution Services In Multiple Basic Trading Areas*, Memorandum Opinion and Order, 13 FCC Rcd 18709, 18714-15, para. 9 (WTB-PSPWD 1998) (emphasis added). We do not accept CUA's suggestion that CUG should be viewed as a minority shareholder of CUA when CUA expressly states that CUG holds 100% ownership of CUA. *See* CUA Response to *Institution Order* at 32; CUA Response to *Order to Show Cause* at 16 & Exh. 2.

[210] *See infra* paras. 53, 55-56.

[211] *See infra* paras. 55, 57.

[212] *See infra* paras. 55, 57-58.

[213] CUA Response to *Institution Order* at 36.

[214] Executive Branch Letter at 20-21 & nn.123, 125 (citing 2020 CUHK SEC Annual Report at 22 ("Our ultimate controlling shareholder is [CU], a company incorporated under the laws of the [People's Republic of China] and majority-owned by the [People's Republic of China] Government."); *id*. at 48). *See* CUA Response to *Institution Order* at 31-33.

[215] *See* CUA Response to *Institution Order* at 32 ("CUG is 100% owned by [CUHK]").

[216] *See* Executive Branch Letter at 20 (quoting 2020 CUHK SEC Annual Report at 22); 2020 CUHK SEC Annual Report at 13; *see* 2021 CUHK SEC Annual Report at 11 ("[CU] indirectly controlled an aggregate of approximately 79.9% of our issued share capital as of April 14, 2021 and all of our five executive directors also concurrently served as directors or executive officers of [CU] as of the same date. As our *ultimate controlling shareholder*, subject to our articles of association and applicable laws and regulations, [CU] is effectively able to control our management, policies and business by controlling the composition of our board of directors and, in turn, indirectly

(continued….)

in its chain of ownership, despite having been explicitly asked to do so by the Commission in the *Institution Order*,[217] does not change our analysis concerning CUA's ownership and control. In fact, CUHK's annual filings with the SEC show that SASAC, and therefore the Chinese government, control both CU and CUHK.[218] The Executive Branch agencies state that CUHK "admitted in its 2020 SEC Annual Report that [CU] could make [CUHK] take actions that conflict with the interests of [CUHK] or its shareholders."[219] As the Executive Branch agencies highlight, "[a]ccording to [CUHK's] 2020 SEC Annual Report, the SASAC may 'request' that [CU] appoint or remove certain individuals as [CUHK's] directors or senior management."[220] This evidence contradicts CUA's arguments and demonstrates that CUA is not independent from CUG, CUHK, CU, and, through SASAC, the Chinese government.

53. CUA contends that it "maintains ultimate control of its day-to-day operations" and that its "board of directors delegates the day-to-day business of the corporation to a person or management of the company as long as the corporation's business and affairs are managed under the ultimate direction of the board."[221] While CUA makes this claim, the record shows that CUA's board of directors have extensive authority over CUA's operations and, based on CUA's June 1, 2020 response to the *Order to Show Cause*, {[

]}[223] Further, as of CUA's

(Continued from previous page)
controlling the selection of our senior management, determining the timing and amount of our dividend payments, approving significant corporate transactions, including mergers and acquisitions, and approving our annual budgets. The interests of [CU] as our ultimate controlling shareholder may conflict with our interests or the interests of our other shareholders. As a result, [CU] may cause us to enter into transactions or take (or fail to take) other actions or make decisions that may not be in our or our other shareholders' best interests." (emphasis added)).

[217] The *Institution Order* directed CUA to provide "a complete and detailed description of the current ownership and control of [CUA], including a description of the equity interest and voting interest for any entity that holds a ten percent or greater direct or indirect interest in and/or controls [CUA]." *Institution Order*, 36 FCC Rcd at 6362, Appx. A. In its response to the *Institution Order*, CUA failed to distinguish between voting and equity interest for each entity in its chain of ownership. CUA also did not describe with specificity the percentages of its ownership attributable to its indirect parent entities, CUHK and CU. Rather, CUA simply stated that it is "100% owned by [CUG]" and that "[o]ther than CUG, no other entity that holds a ten percent or greater direct or indirect ownership interest in and/or controls CUA or has management and oversight of CUA's operations." CUA Response to *Institution Order* at 32, 35; *see supra* note 207.

[218] *See, e.g.*, 2021 CUHK SEC Annual Report at 48, 72, 105; 2020 CUHK SEC Annual Report at 48, 72.

[219] Executive Branch Letter at 21 (citing 2020 CUHK SEC Annual Report at 13 and quoting from CUHK's filing, "[o]ur ultimate controlling shareholder, [CU], can exert influence on us and cause us to make decisions that may not always be in the best interests of us or our other shareholders").

[220] *Id*. (citing 2020 CUHK SEC Annual Report at 48); *see* 2020 CUHK SEC Annual Report at 48 (stating, "the SASAC has an indirect influence over us as our ultimate controlling shareholder, [CU], is under the direct supervision of the SASAC. In particular, the SASAC may designate certain nominees and request [CU] to propose the appointment of such nominees as our directors and senior management. The SASAC may also request [CU] to remove our directors and senior management in accordance with relevant procedures provided by applicable law and our articles of association."); 2021 CUHK SEC Annual Report at 48.

[221] CUA Response to *Institution Order* at 39.

[222] CUA Response to *Order to Show Cause*, Business Confidential Exh. 3.

[223] *Id*.; CUA Response to *Institution Order*, Business Confidential Exh. 1 at 17. *See Institution Order*, 36 FCC Rcd at 6338, para. 29 (stating, "According to the information provided by [CUA], {

]}," and citing CUA Response to *Order to Show Cause*, Business Confidential Exhs. 3, 4).

April 28, 2021 response to the *Institution Order*,[224] {[

]}[225] Given these facts, the record is clear that due to the makeup of the board of directors of CUG, CUA may control its day-to-day business operations, but it would not be independent of any influence from CUG, CU, or ultimately, the Chinese government.

54. We reject CUA's argument that it is wholly independent of its parent entities because it is "a for-profit corporation organized and under the laws of the State of California and subject to the requirements of California corporate law."[226] CUA argues that, because it is a U.S. company subject to the laws of the United States, "there are meaningful protections, in particular in light of private and public shareholders, against improper exercise of control by the Chinese government over CUA's U.S. business

[224] Based on CUA's April 28, 2021 Response, {[

]} CUA Response to *Institution Order*, Business Confidential Exh. 1, at 1-15. According to publicly available information associated with CUHK, three individuals identified in CUA's April 28, 2021 filing as officers, directors, and/or other senior management of CUHK {[ ]} no longer hold those positions at CUHK. China Unicom (Hong Kong) Limited, Resignation of Director (June 11, 2021), https://www1.hkexnews hk/listedco/listco news/sehk/2021/0611/2021061100978.pdf; China Unicom (Hong Kong) Limited, Resignation of Director (June 18, 2021), https://www1 hkexnews.hk/listedco/listconews/sehk/2021/0618/2021061800909.pdf; China Unicom (Hong Kong) Limited, Resignation of Chairman and Chief Executive Officer (Aug. 27, 2021), https://www1 hkexnews.hk /listedco/listconews/sehk/2021/0827/2021082701008.pdf. However, based on CUA's April 28, 2021 response and publicly available information about CUHK's corporate leadership, the three current Executive Directors of CUHK are officers and/or directors of CU. *See* China Unicom (Hong Kong) Limited, List of Directors and their Role and Function (Dec. 3, 2021), https://www1.hkexnews hk/listedco/listconews/sehk/2021/1203/2021120301666.pdf; China Unicom (Hong Kong) Limited, Appointment of Executive Director (Dec. 3, 2021), https://www1.hkex news hk/listedco/listconews/sehk/2021/1203/2021120301638.pdf; China Unicom (Hong Kong) Limited, Appointment of Executive Director, Chairman and Chief Executive Officer as well as Nomination Committee Member (Sept. 3, 2021), https://www1.hkexnews hk/listedco/listconews/sehk/2021/0903/2021090301631.pdf (Sept. 3, 2021 Announcement); 2021 CUHK SEC Annual Report at 65. *See also* CUA Response to *Institution Order*, Business Confidential Exh. 1 at 2. The Chairman and Chief Executive Officer of CUHK is also the Chairman of CU and Chairman of CU A-Share. *See Sept. 3, 2021 Announcement*; China Unicom (Hong Kong) Limited, *Directors and Senior Management—Liu Liehong*, https://www.chinaunicom.com.hk/en/about/bio.php?from=directors& id=liuliehong (last visited Jan. 24, 2022).

[225] CUA Response to *Institution Order*, Business Confidential Exh. 1 at 19-30; CUA Response to *Order to Show Cause*, Business Confidential Exh. 4. *See Institution Order*, 36 FCC Rcd at 6338-39, para. 29 ("{[ ]}, [CUA's] ultimate parent that is majority owned and controlled by the Chinese government.") (citing CUA Response to *Order to Show Cause*, Business Confidential Exh. 4). {[

]} CUA Response to *Institution Order*, Business Confidential Exh. 1 at 19, 27; CUA Response to *Order to Show Cause*, Business Confidential Exh. 4 at 15. {[ ]} CUA Response to *Institution Order*, Business Confidential Exh. 1 at 27; CUA Response to *Institution Order*, Business Confidential Exh. 4 at 15. {

]} CUA Response to *Institution Order*, Business Confidential Exh. 1 at 17; CUA Response to *Order to Show Cause*, Business Confidential Exh. 4 at 11. {]} CUA Response to *Institution Order*, Business Confidential Exh. 1 at 1, 17. *See supra* note 22 (discussing the overlap between the directors and senior executives of CUHK, CU A-Share, and CU).

[226] CUA Response to *Institution Order* at 38 (adding that "the mere fact that CUA is a wholly owned subsidiary of another corporation is not, by itself, sufficient reason to disregard CUA's separate corporate identity").

activities undertaken pursuant to its section 214 authorizations."[227] The Commission already addressed and rejected a similar argument in both the *China Mobile USA Order* and the *China Telecom Americas Order on Revocation and Termination*, finding that an entity's incorporation in the United States does not prevent that entity from being forced to comply with Chinese government requests.[228] As discussed below, CUA failed to provide evidence to rebut the Executive Branch agencies' significant concerns that CUA will be forced to comply with Chinese government requests or to persuade us to depart from our previous assessments with respect to other similarly situated entities.[229]

55. Moreover, the record evidence shows that CUG, CUA's direct parent, oversees important matters involving CUA. Importantly, CUG has significant access to U.S. customer records and control and management of CUA's network operations.[230] For example, according to the PSI Report, CUA "consults with its parent company before establishing any point of presence [(PoPs)] in the United States,"[231] CUG "monitors CUA's network operations," and "CUA also leverages CUG's network operation center [(NOC)], located in Hong Kong, for technical support."[232] The PSI Report also states that "customer records are stored on servers in Hong Kong and maintained by CUG."[233] CUA further informed Congress, but not the Commission, that CUG can remotely configure CUA's network equipment.[234] As we stated in the *Institution Order*, according to the PSI Report, CUG manages CUA's U.S. customer records subject to "a confidentiality agreement that governs access to the records and also establishes procedures to protect customer proprietary network information [(CPNI)]."[235]

---

[227] CUA Response to *Order to Show Cause* at 18. *But see supra* note 21 (describing CUHK's delisting from NYSE).

[228] *China Mobile USA Order*, 34 FCC Rcd at 3368-69, 3371, paras. 16-17, 19; *id*. at para. 19 (stating that the Commission "find[s] China Mobile USA's argument that it is not susceptible to exploitation, influence, and control by the Chinese government because it is incorporated and based in the United States to be unpersuasive. The record does not provide any basis for the contention that China Mobile would not be treated similarly to other Chinese state-owned enterprises or that China Mobile USA itself, as a subsidiary of China Mobile, would not be subject to such control"). *See China Telecom Americas Order on Revocation and Termination* at *19, para. 53 ("CTA fails to refute the evidence in the record that demonstrates it is influenced and controlled in major matters by its direct and indirect parent entities and ultimately subject to influence and control by the Chinese government, notwithstanding that CTA 'is a Delaware corporation.'").

[229] *See infra* paras. 63, 67-72.

[230] *See* CUA Response to *Institution Order*, Business Confidential Exh. 3 at 1-2 ({[ ]}); *Id*., Business Confidential Exh. 4 at 1-2 ({[ ]}). *See also* PSI Report at 78-79 (stating that CUG "appoints CUA's management team, sets CUA's budget, and provides support for technical solutions, among other items.").

[231] PSI Report at 78-79 (citing Briefing with China Unicom Americas (Apr. 16, 2020)); see *Institution Order*, 36 FCC Rcd at 6344, para. 38.

[232] PSI Report at 79 (citing Briefing with China Unicom Americas (Apr. 16, 2020)).

[233] *Id*.

[234] *Id*. (citing Letter from Squire Patton Boggs, counsel to CUA, to the Subcommittee (Apr. 29 2020) (on file with the Subcommittee)).

[235] *Institution Order*, 36 FCC Rcd at 6344, para. 38 (quoting PSI Report at 79 (citing Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee))). We note that in the *Institution Order*, we directed CUA to provide "a detailed response that explains the discrepancies/omissions, as described in [the Institution Order], concerning . . . [CUA's] statements to the [Senate Subcommittee], as described in the PSI Report, and the statements made by [CUA] in response to the *Order to Show Cause*[.]" *Institution Order*, 36 FCC Rcd at 6362. CUA failed to do so with any particularity. In its response to the *Institution Order*, CUA did not fully explain the inconsistencies between its filings with the Commission and its submissions to the Senate Subcommittee that demonstrate that, according to the PSI Report, CUG has greater access to CUA's U.S. records

(continued….)

56. CUA has not proffered any evidence concerning CUA's "governance or decision making" that would persuade us that CUA is independent from CUG or its other parent companies. CUA states that it is governed by its articles of incorporation, adopted in 2010, which "authorize the company to engage in any lawful act or activity for which a corporation may be organized under the General Corporation Law of California."[236] Moreover, CUA points to CUG's Code of Business Conduct (Code) as the only other written policy or agreement that governs CUA's operations.[237] This Code, however, only indicates that CUA and CUG have committed to adhere to the national laws where they operate, including the United States.[238] We find that this Code provides no evidence of CUA's independence from CUG or any other parent entity. The Code is an eight-page document that discusses such topics as {[ ]}[239] The Code {[ ]}[240] CUA, however, failed to provide these documents in the record.[241] Specifically, the Code and CUA's accompanying explanation {[ ]}[242] Accordingly, the Code {[ ]}

(Continued from previous page)
and control over CUA's management than CUA indicated in its response to the *Order to Show Cause*. *See infra* paras. 112-118.

[236] CUA Response to *Institution Order* at 36. CUA states that its Bylaws "provide more detailed provisions of corporate governance, and are typical in form and content for a California corporation." *Id*.

[237] *Id*. ("There are no other written 'policies or agreements' concerning CUAs 'governance or decision making.'"). CUA states that as a matter of its corporate governance or decision making, it "abides by the Code of Business Conduct ('Code') of [CUG], . . . which was adopted in March 2019 to formally document the core principles for making responsible and ethical business decisions" and "reflects [CUG]'s overall commitment to full compliance with the laws of the countries in which it operates, including the United States." *Id*. at 36. *See* CUA Response to *Order to Show Cause* at 31 ("CUG's Code of Business Conduct clearly directs that all of its overseas subsidiaries must operate in compliance with the laws and regulations of the jurisdictions in which they operate. In addition, CUG's policy directs that should any requirements of internal corporate governance codes and policies conflict or be inconsistent with the local laws and regulations of the jurisdictions in which the overseas subsidiaries or members operate, they must first apply and abide by the local laws and regulations."). In the *Institution Order*, the Commission directed CUA to provide "a description and copy of any policies or agreements concerning [CUA's] corporate governance or decision making, including [CUG's] Code of Business Conduct." 36 FCC Rcd at 6362, Appx. A.

[238] CUA Response to *Institution Order* at 36.

[239] *See generally* CUA Response to *Institution Order*, Business Confidential Exh. 2.

[240] *Id*., Business Confidential Exh. 2 at 2-7.

[241] CUA thereby failed to provide the Commission with certain documents that it claims concern its "governance or decision making" and would therefore evince CUA's independence. *See id*. at 36. The absence of these documents, however has no bearing on our ability to determine that CUA is not sufficiently independent from its direct and indirect parent entities.

[242] Moreover, we are not persuaded that this eight-page document is dispositive of CUA's or CUG's "commitment to full compliance with the laws of the countries in which it operates" or of such compliance. *Id*. at 36.

57. The record instead reflects CUA's close affiliation with its direct parent, CUG,[243] and that {[ ]} CUA indicated in its response to the *Order to Show Cause* that CUA's IEPL services rely on CUG's global transmission network.[245] CUA's response at that time did not reflect CUG's extensive and much broader role in CUA's service offerings or management.[246] In its response to the *Institution Order*, CUA states that "CUG provides shared services to CUA, as well as all of its international subsidiaries, for product development, technical solutions, network monitoring and planning, order implementation, project management, and customer services."[247] Further, CUA states that {[ ]}

58. The degree of CUA's parent entities' involvement in CUA is further demonstrated by {[

[243] The *Institution Order* directed CUA to provide "a detailed description of the management and oversight of [CUA] by [CUG] and any entity that holds a ten percent or greater direct or indirect ownership interest in and/or controls [CUA]." *Institution Order*, 36 FCC Rcd at 6362, Appx. A. In its response, CUA failed to provide any detail into CUA's relationship with its other parent entities, CUHK and CU, and instead intimated that only CUG had oversight or management of CUA. Based on the record evidence, CUA also failed to provide the Commission with relevant information concerning CUG's role in CUA's management and operations {[ ]}.

[244] {[ ]} *See infra* note 254.

[245] CUA Response to *Order to Show Cause* at 23.

[246] *See id.* at 20 ("CUG . . . just like common practices of other multinational companies alike, appoints the board members and management team, and approves the annual business plan and budget of CUA.").

[247] CUA Response to *Institution Order* at 35.

[248] *Id.*, Business Confidential Exh. 3 at 1.

[249] *Id.*, Business Confidential Exh. 3 at 1-2.

[250] *Id.*, Business Confidential Exh. 3 at 2.

[251] *Id.*

[252] *Id.*

[253] *Id.*

]} Despite being afforded several opportunities to explain how it is independent from its direct and indirect parent entities, CUA provided inconsistent information that obscures its management {[ ]} Contrary to CUA's claims, we find that the overwhelming evidence in the record shows how integrated CUA's operations—{[ ]} Further, given CUA's failure to provide a complete or accurate response to the Commission's inquiry on these matters[257] or even acknowledge that {[ ]}

59. Further, we reject CUA's argument that the Commission is "piercing CUA's corporate veil and holding it responsible for the actions of its parent entities or indirect owners."[258] CUA argues that by "essentially disregard[ing] CUA's existence as a separate corporate entity [from the Chinese government] and assum[ing] that the [People's Republic of China] government controls it,"[259] the Commission is "piercing the corporate veil" to treat "a carrier, its parent entity, and its ultimate controlling owner as 'one and the same' for legal purposes"[260] contrary to Commission precedent.[261] We

[254] *Id.*, Business Confidential Exh. 3 at 3-6. {

]}

[255] *See generally* CUA Response to *Institution Order*, Business Confidential Exh. 3 at 3-6.

[256] *Id.*, Business Confidential Exh. 4 at 1.

[257] *Institution Order*, 36 FCC Rcd at 6362, Appx. A.

[258] CUA Response to *Institution Order* at 39-40.

[259] *Id.* at 36.

[260] *Id.*

[261] *Id.* at 36-37; *see also* CUA Response to Executive Branch Letter at 12 (arguing that the Executive Branch agencies are wrongfully encouraging the Commission to pierce CUA's corporate veil and stating that, "[o]rdinarily, piercing the corporate veil is appropriate only in unusual circumstances, when a purportedly distinct entity is really (continued….)

disagree. We do not assert that CUA is the same as or a part of the Chinese government, but that the Chinese government could direct CUA, through its parent entities, to take certain actions that would threaten U.S. national security and law enforcement interests. Our finding is based on the public interest analysis under section 214 of the Act and takes into account the significant and substantial national security and law enforcement concerns associated with CUA's ultimate ownership and control by the Chinese government.[262]

60. In line with the Commission's and the Executive Branch agencies' stated concern about the Chinese government's ability to influence state-owned enterprises, and, accordingly, their indirect subsidiaries, through Chinese Communist Party organizations,[263] we find that CUA's parent entities "are likely 'beholden to the [Chinese Communist Party] and appear capable of influencing [CUA] in ways that would satisfy the [Chinese Communist Party's] agenda.'"[264] For instance, as noted in the *Institution Order*, CUA's indirect parent entity, CU, discloses on its website that "[i]n recent years, [it] has insisted on taking political building as the overarching principle and resolutely implemented all major policies and plans of the [Chinese Communist Party] Central Committee."[265] Significantly, the Executive Branch agencies observe that CU stated in its 2018 Social Responsibility Report that "Party leadership has been integrated and embedded into corporate governance and the work requirements for Party building have been included in the Company's regulations, which makes it clear that study and discussion by the Party Leadership Group is a procedure taken before the decision making on major issues by the Board of Directors and the management."[266] CUA did not address this evidence in the record, and we find nothing

(Continued from previous page)
one and the same as its parent or owner, and the companies have behaved as such. . . . As discussed above, there is no evidence, or even a suggestion, that CUA's section 214 authorizations are jeopardizing the 'integrity of the Act' because there is no evidence (or even allegations) of any wrongdoing.").

[262] Even if we were to conduct the Commission's traditional veil-piercing analysis, we would still find that it is appropriate to "disregard CUA's existence as a separate corporate entity" from its direct and indirect parent entities. The three relevant considerations—"(i) where there is a common identity of officers, directors, or shareholders; (ii) where there is common control between the entities; and (iii) when it is necessary to preserve the integrity of the Act and to prevent the entities from defeating the purpose of statutory provisions"—are all present here. *TelSeven, LLC, Patrick Hines*, Forfeiture Order, 31 FCC Rcd 1629, 1631, para. 8 (2016); *see also* CUA Response to *Institution Order* at 36-37. As previously discussed, there exists a common identity of officers and directors that flows among CU, CUHK, CUG, and CUA. *See supra* para. 53 & notes 224, 225. Additionally, the Chinese government, through SASAC, controls CU in CUA's vertical chain of ownership; CU, and indirectly, the Chinese government, control CUHK; CUHK, and indirectly, CU and the Chinese government, control CUG; and CUG, and indirectly, CUHK, CU, and the Chinese government, control CUA. *See* CUA Response to *Institution Order* at 31; *see supra* para. 52 & notes 219, 220. Finally, given the Commission's mandate to protect and promote national security and the Chinese government's history of involvement with espionage and other harmful actions through its state-owned entities, we believe that it would be necessary to preserve the integrity of the Act to pierce the corporate veil in this situation. *See infra* para. 76. Ultimately, however, we hold that it is not necessary to do so.

[263] *See China Telecom Americas Order on Revocation and Termination* at *19, *20-22, paras. 51, 54-60; *China Mobile USA Order*, 34 FCC Rcd at 3369-70, para. 18.

[264] *Institution Order*, 36 FCC Rcd at 6337, para. 28 (quoting Executive Branch Letter at 25); *see id*. at 6337, n.117 (citing Executive Branch Letter at 23-24 and quoting the Executive Branch agencies' statements that "members of the [Chinese Communist Party] run both [CU] and [CUHK]" and that CU "has repeatedly proclaimed that it serves the [Chinese Communist Party]"); Executive Branch Letter at 23-25.

[265] *See Institution Order*, 36 FCC Rcd at 6337, n.117 (quoting China United Network Communications Group Co., Ltd., *About*, http://www.chinaunicom.com.cn/about/about html); China United Network Communications Group Co., Ltd., *About,* http://www.chinaunicom.com.cn/about/about html (last visited Jan. 26, 2022).

[266] China United Network Communications Group Company Limited, Social Responsibility Report of 2018 at 7 (Aug. 5, 2018), https://www.unglobalcompact.org/participation/report/cop/create-and-submit/active/428529 (CU Social Responsibility Report); *see* Executive Branch Letter at 24 (quoting CU Social Responsibility Report at 7);
(continued….)

in the record to refute these concerns. Moreover, there is no evidence in the record to show that CUA has measures in place to counter the strong presence of Chinese Communist Party influence within CUA's indirect parent entities that "make[s] CUA vulnerable to direct exploitation by the [Chinese Communist Party]."[267]

61. Additionally, our concerns with CUA's ownership and control by the Chinese government are concordant with concerns that we previously addressed regarding the influence of the Chinese Communist Party and, consequently, the Chinese government over other Chinese state-owned entities and their U.S. subsidiaries and the threats that the retention of section 214 authority by such subsidiaries pose to the United States.[268] For instance, in the *China Telecom Americas Order on Revocation and Termination*, we stated that national security and law enforcement concerns "stem from the integrated presence and the extent of influence of the Chinese Communist Party, including in military and economic sectors,"[269] and that "[t]he U.S. government has found that the Chinese government exerts influence over state-owned enterprises through the Chinese Communist Party."[270] Further, we

(Continued from previous page)
Institution Order, 36 FCC Rcd at 6337-38 (citing Executive Branch Letter at 24). *See* CU Social Responsibility Report at 18 ("Guided by Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, [CU] earnestly implemented the general requirements for Party building in the new era, put political construction in a leading position, adhered to and enhanced the overall leadership of the Party, as well as strived to consolidate its base and root and build the soul, through which the Party building quality in the Company has improved comprehensively."); *Institution Order*, 36 FCC Rcd at 6337-38, para. 28 & n.118 (quoting CU Social Responsibility Report at 18).

[267] *See* Executive Branch Letter at 22.

[268] *See*, *e.g.*, *China Telecom Americas Order on Revocation and Termination* at *22, para. 59.

[269] *Id.* at para. 59 & n.251 (citing Executive Branch CTA Recommendation, Exh. 113 at EB-2379-83, Full text of resolution on amendment to CPC Constitution, State Council of the People's Republic of China, http://english.www.gov.cn/news/top_news/2017/10/24/content_281475919837140.htm (Oct. 24, 2017) (Resolution on the Revised Constitution of the Communist Party of China); *id.*, Exh. 114 at EB-2384-2411, Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress (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)). The Revised Constitution of the Communist Party of China states, among other things, that "[t]he Communist Party of China shall uphold its absolute leadership over the People's Liberation Army and other people's armed forces . . . and pursue the Belt and Road Initiative." Revised Constitution of the Communist Party of China at 7-8 ("General Program"); *China Telecom Americas Order on Revocation and Termination* at *22, para. 59, n.251 (citing Executive Branch CTA Recommendation, Exh. 113 at EB-2381, Resolution on the Revised Constitution of the Communist Party of China); *see* Executive Branch Response to December 10, 2020 Order Instituting Proceedings on Revocation and Termination and Memorandum Opinion and Order, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, at 13 (filed Jan. 14, 2021) (Executive Branch CTA Response) (stating, "[t]he U.S. intelligence community has raised particular concerns about the Belt and Road Initiative, citing its potential to extend the [Chinese] military's global reach" and citing Executive Branch CTA Recommendation, Exh. 8 at EB-371, *Worldwide Threat Assessment of the U.S. Intelligence Community: Before the S. Select Comm. On Intelligence*, 116th Cong. at 25 (2019) (statement of Daniel R. Coats, Director of National Intelligence), https://go.usa.gov/xe7ht (2019 Worldwide Threat Assessment by the Director of National Intelligence)); *China Telecom Americas Order on Revocation and Termination* at *22, para. 59, n.251 (citing Executive Branch CTA Response at 13).

[270] *China Telecom Americas Order on Revocation and Termination* at *22, para. 59. The *China Telecom Americas Order on Revocation and Termination* noted, for example, the assessment of USTR's 2018 Report on Findings of the Investigation into China's Acts, Policies, and Practices that "[t]he guiding principles for government ownership and control are set forth in the Constitution of the People's Republic of China . . . and the [Chinese Communist Party] Constitution" and that "[t]hrough the [Chinese Communist Party], the Chinese government exercises additional control over [state-owned enterprise] behavior." *Id.* (quoting Executive Branch CTA Recommendation, Exh. 60 at EB-1063, 1066, 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, Office of
(continued….)

acknowledged the Executive Branch agencies' observation that, "[a]ccording to the Chinese government, the [amendments to the Revised Constitution of the Communist Party of China] were made to 'define the status and role of Party organizations in State-owned enterprises.'"[271] In the *Institution Order*, we recognized that under Article 32 of the Revised Constitution of the Communist Party of China, "[p]rimary-level Party organizations play a key role for the Party in the basic units of social organization" and 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."[272] We noted that 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."[273] Further, as we also stated in the *Institution Order*, Article 19 of the Company Law of the People's Republic of China (2018 Amendment) states that "[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," and that "[t]he company shall provide necessary conditions to facilitate the activities of the Party."[274] Given the evidence in the record, we agree with the Executive Branch agencies that "the entities that control [CUA] and its direct parent [CUG] are likely 'beholden to the [Chinese Communist Party] and appear capable of influencing [CUA] in ways that would satisfy the [Chinese Communist Party's] agenda.'"[275]

(Continued from previous page)
the U.S. Trade Representative, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF (2018) (USTR Section 301 Report)). We also noted the analysis of the USTR Section 301 Report in the *Institution Order*. *See Institution Order*, 36 FCC Rcd at 6337, n.116 (citing USTR Section 301 Report at 81, n.446 and noting from the Report 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").

[271] *See China Telecom Americas Order on Revocation and Termination* at *22, para. 59 (quoting Executive Branch CTA Recommendation at 36 and noting citation to *id.*, Exh. 113 at EB-2382, Resolution on the Revised Constitution of the Communist Party of China); *see id.* at *20, para. 54; *see supra* note 269. We also noted that "[a]ccording to Article 33 of the Revised Constitution, '[p]rimary-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.'" *China Telecom Americas Order on Revocation and Termination* at *22, para. 59 (quoting Executive Branch CTA Recommendation, Exh. 114 at EB-2404, Revised Constitution of the Communist Party of China); *see Institution Order*, 36 FCC Rcd at 6337, n.117 (quoting Revised Constitution of the Communist Party of China, Article 33).

[272] Revised Constitution of the Communist Party of China, Article 32; *Institution Order*, 36 FCC Rcd at 6337-38, n.117 (quoting Revised Constitution of the Communist Party of China, Article 32).

[273] Revised Constitution of the Communist Party of China, Article 33; *Institution Order*, 36 FCC Rcd at 6337, n.117 (quoting Revised Constitution of the Communist Party of China, Article 33).

[274] Law of China, Company Law of the People's Republic of China (2018 Amendment), Article 19, http://lawinfochina.com/display.aspx?id=e797dd968c30e172bdfb&lib=law (Company Law of the People's Republic of China (2018 Amendment)); *Institution Order*, 36 FCC Rcd at 6338, n.117 (quoting Company Law of the People's Republic of China (2018 Amendment), Article 19).

[275] *Institution Order*, 36 FCC Rcd at 6337, para. 28 (quoting Executive Branch Letter at 25). In its response to the *Order to Show Cause*, CUA argues that "CUG and CUA should not be presumed to be at risk of becoming not law abiding solely due to the fact that certain directors of CUG are Chinese Communist Party ('CCP') members. If they are so presumed, that is simple discrimination based on political affiliation. Even if all Mainland directors of CUG are members of CCP, it does not necessarily follow that CUA will not comply with U.S. laws." CUA Response to the *Order to Show Cause* at 21-22. Our determination that the presence of Chinese Communist Party influence over {[ ]} CUA presents significant risks does not rest on "simple discrimination based on political affiliation." Rather, we take into account {[

(continued….)

62. We find based on the record that the Chinese government has the ability to influence CUA through the significant and irrefutable ties of its corporate leadership and that of its parent entities with the Chinese Communist Party. As we noted above, {[

]}[279] Not only does this information undermine CUA's argument that it is independent from these entities, but it also demonstrates {[

]}[280] Accordingly, we agree with the Executive Branch agencies' statement that the potential for Chinese Communist Party influence "is not theoretical."[281] The record evidence also shows how CU '"has further demonstrated its support of the [Chinese Communist Party] agenda through its activities in the Xinjiang Autonomous Region,' in which '[t]he [Chinese] government is conducting a campaign against Uyghurs, ethnic Kazakhs, Kyrgyz, and members of other Muslim minority groups in the Xinjiang Uyghur Autonomous Region through high-tech mass surveillance and arbitrary detention.'"[282] CUA has provided no evidence to refute CU's close ties to the Chinese government or to

(Continued from previous page)

]} in conjunction with CU's support of the Chinese Communist Party and CU's integration of Chinese Communist Party ideals and priorities into its operations. *See supra* paras. 60-61.

[276] CUA Response to *Order to Show Cause*, Business Confidential Exh. 3; *see supra* para. 53.

[277] CUA Response to *Institution Order*, Business Confidential Exh. 1 at 17; CUA Response to *Order to Show Cause*, Business Confidential Exh, 3. *See Institution Order*, 36 FCC Rcd at 6338, para. 29 ("According to the information provided by [CUA], {[

]}") (citing CUA Response to *Order to Show Cause*, Business Confidential Exhs. 3, 4); *see supra* para. 53.

[278] CUA Response to *Institution Order*, Business Confidential Exh. 1, at 1-15. We note that when the Commission first asked CUA to provide "an identification of all officers, directors, and other senior management of entities that hold ten percent or greater ownership interest in [CUA], their employment history (including prior employment with the Chinese government), and their affiliations with the Chinese Communist Party and the Chinese government," CUA only provided this information with respect to CUG, and not any other entity that holds ten percent or greater ownership in CUA, even though CUA indicated that entities with such ownership interests include, at a minimum, CUHK and CU. *See Institution Order*, 36 FCC Rcd at 6338, n.119 (citing *Order to Show Cause*, 35 FCC Rcd at 3725, para. 9); *Order to Show Cause*, 35 FCC Rcd at 3725, para. 9.

[279] CUA Response to *Institution Order*, Business Confidential Exh. 1, at 19-30; *see Institution Order*, 36 FCC Rcd at 6338, para. 28 ({

]}); CUA Response to *Order to Show Cause*, Business Confidential Exh. 4.

[280] *See* CUA Response to *Order to Show Cause*, Business Confidential Exh. 3.

[281] Executive Branch Letter at 25; *see id.* at 22-25 (stating that CUA is "duty bound to follow [Chinese Communist Party] priorities and goals" and explaining that "[t]he [Chinese Communist Party's] influence over [CU] and [CUHK], which indirectly own and control CUA, make CUA vulnerable to direct exploitation by the [Chinese Communist Party]"); *Institution Order*, 36 FCC Rcd at 6339, para. 30.

[282] *Institution Order*, 36 FCC Rcd at 6339, para. 30 (quoting Executive Branch Letter at 25 (citing Uyghur Human Rights Policy Act of 2020, Pub L. No. 116-145, 134 Stat. 648, Section 3 (June 17, 2020))); *see id.* at n.125.

counter the evidence demonstrating that CU works to further the ideals and priorities of the Chinese Communist Party and the Chinese government.[283]

63. Moreover, CUA has proffered no evidence to demonstrate that CU, as a state-owned enterprise, is situated differently from other Chinese state-owned enterprises that the Commission has already found to be able to exert influence and control over their U.S.-based subsidiaries. As we indicated in the *Institution Order*, the record shows "the close ties between China Unicom, China Mobile Communications Group Co., Ltd (China Mobile), and China Telecommunications Corporation (China Telecom)," including the fact that "although the three entities are 'technically competitors,' they 'collaborate on projects at the government's discretion.'"[284] This validates the Executive Branch agencies' contention that, "[f]or purposes of [Chinese] government control, [CU] is indistinguishable from other [Chinese] SOEs, China Mobile and China Telecom,"[285] and thus, the Commission's concerns with respect to those entities apply here as well.[286] We therefore find, as we did with respect to China Mobile USA and China Telecom Americas, that through a Chinese state-owned enterprise's indirect ownership of CUA, the Chinese government is able to exert influence and control over CUA.[287]

a. Chinese Laws May Cause CUA to Be Forced to Carry Out Certain Activities that are Harmful to U.S. Interests

64. The Executive Branch agencies contend, and we agree, that "the Chinese government's majority ownership and control of [CUA] and its direct and indirect parent entities, in addition to Chinese intelligence and cybersecurity laws, 'raise significant concerns that [CUA] will be forced to comply with [Chinese] government requests, including requests for communications intercepts, without the ability to

[283] *See* Executive Branch Letter at 22-26. Further, the Executive Branch Letter explains that "[i]n March 2015, China's National Development and Reform Commission (NDRC), Ministry of Foreign Affairs, and Ministry of Commerce jointly released the Belt and Road white paper," which, among other things, calls for "'jointly improving the transparency of technical trade measures' and creating an 'Information Silk Road,' or a digital Silk Road." *Id*. at 12-13 & n.64 (citing Stewart M. Patrick, Council on Foreign Relations, *Belt and Router: China Aims for Tighter Controls with Digital Silk Road* (July 2, 2018), https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road); *id*. at 21-22 (noting that CU asserted in its 2018 Social Responsibility Report that "[CU] has been implementing the 'Belt & Road' ('B&R') initiative in depth . . . We have set up over 30 *branches* around the world to provide domestically and internationally integrated, global end-to-end comprehensive package information services to global customers and global voice and data services to individual customers abroad" (emphasis added)); *see supra* para. 61 & note 270 (citing, e.g., Revised Constitution of the Communist Party of China at 7-8 ("General Program")). CUA never responded to the Executive Branch agencies' arguments concerning CU's implementation of the Belt and Road Initiative.

[284] *Institution Order*, 36 FCC Rcd at 6339, para. 30 (quoting Executive Branch Letter at 26). Based on the record, we are persuaded by the Executive Branch agencies' argument that "[CU] has such close ties to China's other two main majority state-owned telecoms, China Mobile and China Telecom, that it is unreasonable to assume it would behave differently. . . . They also collaborate on the world stage to export [Chinese] values: [CU], along with China Telecom, Huawei, and China's Ministry of Industry and Information Technology recently jointly proposed to the United Nations International Telecommunications Union to replace [Border Gateway Protocol (BGP)] routing with 'New IP,' a system that would centralize control of the Internet with governments and allow for the issuance of 'shut up command[s]' that would [cut off communication to or from a particular [IP] address.'" Executive Branch Letter at 26-27 (quoting Anna Gross and Madhumita Murgia, *Inside China's controversial mission to reinvent the internet*, Financial Times Magazine (Mar. 27, 2020), https://www ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f); *see Institution Order*, 36 FCC Rcd at 6339, para. 30 & n.127.

[285] Executive Branch Letter at 26.

[286] *See generally China Telecom Americas Order on Revocation and Termination*; *China Mobile USA Order*.

[287] *China Telecom Americas Order on Revocation and Termination* at *17-24, paras. 45-64 (Section III.B.1.); *China Mobile USA Order*, 34 FCC Rcd at 3368-71, paras. 14-19 (Section III.B).

challenge such requests.'"[288] This determination is based on our finding that the Chinese government has influence and control over CUA and its direct and indirect parent entities through, among other things, CUA's ties with the Chinese Communist Party and the requirements of Chinese laws that have been enacted in recent years.[289] Specifically, we find that the 2017 Cybersecurity Law and 2017 National Intelligence Law, as indicated by the Executive Branch agencies, "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."[290] We also find persuasive the Executive Branch agencies' argument that "provisions of China's 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 agencies.'"[291]

65. The Executive Branch agencies raise a number of arguments with respect to their contention that "CUA will have to comply with [Chinese] government requests without sufficient legal procedures subject to independent judicial oversight."[292] With respect to China's 2017 National Intelligence Law, we agree, as discussed below, with the Executive Branch agencies' assessment that this law "provides [Chinese] intelligence services with greater powers to compel Chinese citizens and organizations 'to cooperate, assist, and support Chinese intelligence efforts *wherever they are in the world*.'"[293] Moreover, the Executive Branch agencies argue that China's 2017 Cybersecurity Law and its 2018 implementing regulation (2018 Cybersecurity Regulation)[294] "impose more specific obligations for

[288] *Institution Order*, 36 FCC Rcd at 6340, para. 31 (quoting Executive Branch Letter at 27).

[289] *See id.* at 6340-41, paras. 31-32; Executive Branch Letter at 27-30; *China Telecom Americas Order on Revocation and Termination*, at *22, para. 60.

[290] *See* Executive Branch Letter at 27-28 (citing Dangerous Partners: Big Tech and Beijing: Hearing Before the Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, 116th Congress (Mar. 4, 2020) (statement of Deputy Assistant Attorney General Adam S. Hickey, National Security Division, U.S. Department of Justice), https://www.judiciary.senate.gov/imo/media/doc/Hickey%20Testimony.pdf (Statement of Deputy Assistant Attorney General Adam S. Hickey)); *Institution Order*, 36 FCC Rcd at 6340, para. 31.

[291] *Institution Order*, 36 FCC Rcd at 6340, para. 31 (quoting Executive Branch Letter at 28 (citing Statement of Deputy Assistant Attorney General Adam S. Hickey)).

[292] *See* Executive Branch Letter at 27-30.

[293] *Id*. at 28 (quoting *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 (emphasis added)); *see Institution Order*, 36 FCC Rcd at 6340, n.131 (citing Carolina Dackö and Lucas Jonsson, *Applicability of National Intelligence Law to Chinese and non-Chinese Entities*, Mannheimer Swartling (Jan. 2019), https://www.mannheimerswartling.se/globalassets/nyhetsbrev/msa_nyhetsbrev_national-intelligence-law_jan-19.pdf; National Intelligence Law of the People's Republic, National People's Congress, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (last visited Jan. 26, 2022) (Google's cache of http://www.npc.gov.cn/npc/xinwen/201706/27/content_2024529 htm). The Executive Branch agencies note, in particular, that in the *China Mobile USA Order*, the Commission stated, "Article 7 of the 2017 National Intelligence Law provides 'an organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows.' Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, including communications equipment." Executive Branch Letter at 28 (quoting *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17); *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17 (citing English-language translation at pkulaw.cn, National Intelligence Law of the People's Republic of China (2018 Amendment), http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law (last visited Jan. 26, 2022)).

[294] Executive Branch Letter at 29 (stating, "[t]he consequences of this 2017 Cybersecurity Law is clarified in the implementing regulation, the November 1, 2018 'Regulation on Internet Security Supervision by Public Security Organs' (Order No. 151 of the Ministry of Public Security)") (citing *China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*, Library of Congress (Nov. 13, 2018), https://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-

(continued….)

telecommunications systems operators, even if they are not state owned."[295] The Executive Branch agencies argue that because the 2017 Cybersecurity Law defines the term "'[n]etwork operators'" broadly as "'network owners, network managers, and network service providers,'"[296] this definition is vague enough to "ensnare[] both foreign and Chinese network operators that own or manage a network or provide online services anywhere within China."[297] Additionally, the Executive Branch agencies point to the 2018 Cybersecurity Regulation, which "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," with the People's Armed Police "present at inspections to ensure compliance with the inspection."[298]

66. CUA contends that it "does not agree that the Chinese laws referenced by the Commission in [the *Institution Order*] obligate CUA to comply with requests from the Chinese government."[299] Specifically, CUA argues that the 2017 Cybersecurity Law, the 2017 National Intelligence Law, and the 2019 Cryptography Law or their associated implementing regulations do not "mandate CUA compliance with Chinese government requests as asserted by the [*Institution Order*]."[300] First, CUA argues that "[t]he plain language of the 2017 Cybersecurity Law limits itself to the 'mainland territory of the People's Republic of China ['PRC']," and that "[i]t focuses on regulating activities in the mainland (e.g., construction, operation, maintenance, and use) rather than entities overseas."[301] CUA argues that the same is true of "one of the implementation rules of the [2017 Cybersecurity Law], Internet Security Regulation."[302] CUA argues that the purpose of the 2017 Cybersecurity Law "is to protect China's cybersecurity, rather than provide a vehicle for threatening or endangering the security of other countries' networks."[303] Second, CUA maintains that "there is no indication that the 2017 National

(Continued from previous page)
inspection-powers-issued/; *China's New Cybersecurity Measures Allow State Policy to Remotely Access Company Systems*, Recorded Future Blog (Feb. 8, 2019), https://www.recordedfuture.com/china-cybersecurity-measures/) (*China's New Cybersecurity Measures*)); *see Regulation on Internet Security Supervision and Inspection by Public Security Organs*, http://www.gov.cn/zhengce/zhengceku/2018-12/31/content_5428637.htm (last visited Jan. 26, 2021); *see* Law of China, Provisions on Internet Security Supervision and Inspection by Public Security Organs (Translation), https://www.lawinfochina.com/display.aspx?id=f37b0d2a40065436bdfb&lib=law (last visited Jan. 26, 2022).

[295] Executive Branch Letter at 28; *see Institution Order*, 36 FCC Rcd at 6340, para. 32.

[296] 2017 Cybersecurity Law, Article 76(3) (providing definition of "Network operators" as "network owners, managers, and network service providers"); Executive Branch Letter at 28-29 & n.167 (citing Rogier Creemers, Paul Triolo, and Graham Webster, Translation: Cybersecurity Law of the People's Republic of China, 2017 Cybersecurity Law, Article 76(3) (Effective June 1, 2017), New America (June 29, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/ (2017 Cybersecurity Law)).

[297] Executive Branch Letter at 29 (citing 2017 Cybersecurity Law, Article 2; *White Paper: Implementing China's Cybersecurity Law*, Jones Day (Aug. 2017), https://www.jonesday.com/en/insights/2017/08/implementing-chinas-cybersecurity-law).

[298] *Id*. (citing *China's New Cybersecurity Measures*); *see Institution Order*, 36 FCC Rcd at 6340-41, para. 32.

[299] CUA Response to *Institution Order* at 22.

[300] *Id*. at 23.

[301] *Id*.

[302] *Id*.

[303] *Id*. at 24. CUA cites Article 30 of the 2017 Cybersecurity Law to support its assertion and argues that "neither the Commission nor the Executive Branch agencies mentioned Article 30 of the Cybersecurity Law, which limits the use of any information obtained to the protection of Chinese cybersecurity: 'Information obtained by cybersecurity and information departments and relevant departments performing cybersecurity protection duties can only be used

(continued….)

Intelligence Law has extraterritorial applicability."[304] CUA contends that the 2017 National Intelligence Law "applies only to Chinese citizens and organizations" and that "[t]he Law also places limitations on the conduct of national intelligence efforts."[305] Third, with respect to the 2019 Cryptography Law, CUA argues that "the Executive Branch agencies stated that the Law imposed requirements that will expose commercial encryption used 'within China' to testing and certification by the Chinese government" and that "[i]t is unclear how this would apply to CUA, which is not located within China."[306]

67. Contrary to CUA's contentions, we find that the combination of these laws—the 2017 Cybersecurity Law, the 2018 Cybersecurity Regulation, the 2017 National Intelligence Law, and the 2019 Cryptography Law—raises serious and significant national security risks. We find that the record supports the Executive Branch agencies' assessment that CUA and its parent entities are vulnerable to Chinese government requests based on the requirements of these laws. As an initial matter, with respect to the 2017 Cybersecurity Law, we conclude that this law gives the Chinese government authority over the operations of CUA's parent entities.[307] As we found in another proceeding, we are persuaded by the Executive Branch agencies' legal conclusion that the 2017 Cybersecurity Law "requires extensive cooperation by telecom and network operators" with the Chinese government.[308] The Executive Branch

(Continued from previous page)
as necessary for the protection of cybersecurity, and must not be used in other ways.'" *Id*. (quoting 2017 Cybersecurity Law, Article 30); *see* 2017 Cybersecurity Law, Article 30 ("Information obtained by cybersecurity and informatization departments and relevant departments performing cybersecurity protection duties can only be used as necessary for the protection of cybersecurity, and must not be used in other ways."). CUA further claims that Article 73 of the 2017 Cybersecurity Law "requires the imposition of sanctions upon persons who violate Article 30." *Id*. (citing 2017 Cybersecurity Law, Article 73). CUA neglects to clarify, however, that the full statement of Article 73 specifically states, "[w]here cybersecurity and informatization and other relevant departments violate the provisions of Article 30 of this Law *by using personal information acquired while performing cybersecurity protection duties for other purposes*, the directly responsible persons in charge and other directly responsible personnel shall be given sanctions. Where cybersecurity and informatization departments and other relevant departments' personnel neglect their duties, abuse their authority, show favoritism, and it does not constitute a crime, sanctions will be imposed in accordance with law." 2017 Cybersecurity Law, Article 73 (emphasis added).

[304] CUA Response to *Institution Order* at 24.

[305] *Id*. at 24-25 (citing China Law Translate, National Intelligence Law of the P.R.C., Article 8 (2017) (Passed on June 27, 2017), https://www.chinalawtranslate.com/en/national-intelligence- law-of-the-p-r-c-2017/ (China Law Translate, 2017 National Intelligence Law). CUA argues, by citing Article 8 of the 2017 National Intelligence Law, that the Commission failed to consider that national intelligence efforts "must be conducted in accordance with the law, shall respect and protect human rights, and shall preserve the lawful rights and interests of individuals and organizations." *Id*. at 25 (citing China Law Translate, 2017 National Intelligence Law, Article 8). CUA, however, offers no rebuttal to the Executive Branch agencies' assertion that "the Uyghur Human Rights Policy Act of 2020 . . . found, among other things, that: '[s]enior Chinese Communist Party officials . . . bear direct responsibility for gross human rights violations committed against Uyghurs, ethnic Kazakhs, Kyrgyz, and members of other Muslim minority groups,'" and the evidence in the record demonstrating that "[CU] has responded to [Chinese] government tasks in Xinjiang for years." Executive Branch Letter at 25-26; *see supra* para. 62.

[306] CUA Response to *Institution Order* at 25.

[307] *See Institution Order*, 36 FCC Rcd at 6341, para. 33; Executive Branch Letter at 27-30 (discussing that "CUA's parent entities are governed by these [Chinese] laws"); *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60.

[308] Executive Branch Letter at 28; *see supra* para. 65 & note 297 (discussing "network operators"); *see China Telecom Americas Order on Revocation and Termination* at *22 para. 60 & n.265 (quoting Executive Branch CTA Recommendation at 38-39). Further, Article 35 of the 2017 Cybersecurity Law states that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council." 2017 Cybersecurity Law, Article 35; *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60 (quoting Executive Branch CTA Recommendation, Exh. 51 at EB-876,
(continued….)

agencies further state, for example, that Article 28 of the 2017 Cybersecurity Law states, "[n]etwork operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[309] Additionally, Article 49 of the 2017 Cybersecurity Law states that "[n]etwork operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law."[310] Moreover, as noted by the Executive Branch agencies,"[CU] and [CUHK] have acknowledged being subject to [Chinese] cyber and national security laws,"[311] and "[CUHK] further acknowledged oversight by the [Chinese] government's security services."[312] The Executive Branch agencies assert that "[CUHK] also needs [Chinese] government-issued licenses and approvals to operate, and the majority of its operations, assets, and executives are located in the [People's Republic of China]."[313]

(Continued from previous page)
2017 Cybersecurity Law, Article 35). Additionally, Article 8 of the 2017 Cybersecurity Law states that "[t]he State Council departments for telecommunications, public security, and other relevant organs, are responsible for cybersecurity protection, supervision, and management efforts within the scope of their responsibilities, in accordance with the provisions of this Law and relevant laws and administrative regulations." 2017 Cybersecurity Law, Article 8; *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60, n.265 (quoting Executive Branch CTA Recommendation, Exh. 51 at EB-869, 2017 Cybersecurity Law, Article 8).

[309] 2017 Cybersecurity Law, Article 28; Executive Branch Letter at 28 (quoting 2017 Cybersecurity Law, Article 28).

[310] 2017 Cybersecurity Law, Article 49; Executive Branch Letter at 29 (quoting 2017 Cybersecurity Law, Article 49); *see China Telecom Americas Order on Revocation and Termination* at *22, para. 60 (quoting Executive Branch CTA Recommendation, Exh. 51 at EB-880, 2017 Cybersecurity Law, Article 49).

[311] Executive Branch Letter at 29-30. The Executive Branch agencies observe that CU affirmed in its 2018 Corporate Social Responsibility Report, that "'[CU] has carefully put into practice the spirit and important instruction of "no national security exists if there is no network security" of General Secretary Xi Jinping, and the requirements of the national cybersecurity and information working conference, *strictly implemented the Cybersecurity Law*, and issued a series of business and system security management measures to escort the smooth and steady development of the Company's work in cyber and information security.'" *Id.* at 30 (quoting CU Social Responsibility Report of 2018 at 41 (emphasis added)). Additionally, CUHK acknowledged "that it is subject to the June 1, 2017 Cyber Security Law and the 2018 Information Security Technology—Personal Information Security Specification, which 'set[] forth detailed guidelines on the collection, utilization and retention of personal information and privacy protection.'" *Id.* (citing 2020 SEC Annual Report at 37); *see id.* at 12 (stating, "personal privacy, information security, and data protection are increasingly significant issues in China and other jurisdictions in which we operate. In China, the regulatory framework governing the collection, processing, storage and use of business information and personal data is rapidly evolving. For example, the Cybersecurity Law sets forth the general framework regulating network products, equipment and services, as well as the operation and maintenance of information networks, the protection of personal data, and the supervision and administration of cybersecurity in China"); *see* 2021 CUHK SEC Annual Report at 10.

[312] Executive Branch Letter at 30 (citing 2020 SEC Annual Report at 36). In its Form 20-F filed with the SEC for the fiscal years ended December 31, 2019 and December 31, 2020, CUHK stated, in addressing "Regulatory and Related Matters," that "*[w]e are subject to the Cybersecurity Law, which came into effect on June 1, 2017*" and "[a]ccording to the Cybersecurity Law, the Cyberspace Administration of China, or the CAC, has a central role in planning, coordination, supervision, and management of network security measures while the [Ministry of Industry and Information Technology], the national public safety bureau, and other relevant authorities are in charge of network security protection, supervision and management within the scope of their respective responsibilities." 2020 CUHK SEC Annual Report at 36 (emphasis added); 2021 CUHK SEC Annual Report at 37 (emphasis added).

[313] Executive Branch Letter at 27 (citing 2020 CUHK SEC Annual Report at 16, 19); *see* 2020 CUHK SEC Annual Report at 16 ("Substantially all of our business operations are conducted in China and substantially all of our revenue is derived from our operations in China. Accordingly, our business, financial condition, results of operations and prospects may be adversely affected by changes in China's economic, political and social

(continued….)

68. CUA does not dispute the record evidence demonstrating that CUA's and CUG's parent entities acknowledge that they are subject to the 2017 Cybersecurity Law,[314] and offers no argument that CU or CUHK could not influence or control their subsidiaries to take action based on this law. Instead, CUA contends that CUG, the direct parent of CUA and thus another subsidiary of CU and CUHK, "incorporated in Hong Kong, does not conduct any network business in the [People's Republic of China]; all of its activities are conducted in Hong Kong or elsewhere."[315] We are not persuaded by CUA's contention that "the Cybersecurity Law as well as all the other Chinese laws referred by the Commission do not apply to entities incorporated under the Hong Kong laws and in the territory of Hong Kong."[316] We find, as noted by the Executive Branch agencies in another proceeding, that the combination of these cybersecurity and intelligence laws enhances the Chinese government's ability to access information "entering Chinese territory or traveling through Chinese-owned or -controlled infrastructure outside of China."[317] Additionally, CUA offers no persuasive argument or evidence to refute the Executive Branch agencies' observation that "[CU] does not treat its foreign subsidiaries, including CUA, as independent

(Continued from previous page)
conditions . . . our financial condition and results of operations may be materially and adversely affected by government control over outbound investment"); 2020 CUHK SEC Annual Report at 18.

[314] *See, e.g.,* CU Social Responsibility Report of 2018 at 41; 2020 CUHK SEC Annual Report at 12; 2021 CUHK SEC Annual Report at 10. CUA does not dispute, for example, that its indirect parent CUHK, an entity incorporated in Hong Kong, expressly stated in its filings with the SEC that it "primarily conduct[s] [its] business in Mainland China" and that it is "subject to the Cybersecurity Law, which came into effect on June 1, 2017." 2020 CUHK SEC Annual Report at 10, 36; 2021 CUHK SEC Annual Report at 8, 37.

[315] CUA Response to *Institution Order* at 24, n.104; *but see supra* note 314.

[316] CUA Response to *Institution Order* at 24, n.104. CUA claims that "[i]n case the Chinese government makes any formal request or investigation based on the Cybersecurity Law, the request and investigation scope is only limited to the Network Business in the [People's Republic of China]." *Id.* at 23 (suggesting, "[f]or instance, if a Chinese entity has Network Business both in the [People's Republic of China] and overseas, only the part of Network Business in the [People's Republic of China] is subject to the provisions of the Cybersecurity Law, while the overseas component of its Network Business is not governed by the Cybersecurity Law. Similarly, if a foreign entity has Network Business both in its home state and the [People's Republic of China], only the part of Network Business in the [People's Republic of China] is governed by the Cybersecurity Law, while its Network Business in its own home state falls outside the scope of the Cybersecurity Law.").

[317] *See* Executive Branch Recommendation for a Partial Denial and Partial Grant of the Application for a Submarine Cable Landing License for the Pacific Light Cable Network (PLCN), File Nos. SCL-LIC-20170421-00012; SCL-AMD-20171227-00025; SCL-STA-20180907-00033; SCL-STA-20190327-00011; SCL-STA-20190906-00032; SCL-STA-20200129-00006; SCL-STA-20200313-00014, SCL-STA-20200402-00015, at 24 (filed June 17, 2020) (Executive Branch PLCN Recommendation); *see id.* at 26-27 ("The 2017 Intelligence Law, if applied in concert with the 2017 Cybersecurity Law, provides the [People's Republic of China] government far more specific authority to access and regulate many features of corporate networks (inside as well as outside of China) that might be useful for intelligence gathering."); *see* Chinalawinfo Co. Ltd., Cybersecurity Law of the People's Republic of China (Translation), https://www.lawinfochina.com/display.aspx?id=22826&lib=law&SearchKeyword=cybersecurity%20law&SearchCKeyword= (last visited Jan. 26, 2022); 2017 National Intelligence Law, Articles 7, 14, 17. To the extent CUA refers to the Basic Law of Hong Kong Special Administrative Region of the PRC (1997) (Basic Law), we note that the Executive Branch agencies previously stated in another proceeding that "[a]lthough the Basic Law sets forth the general principle that [People's Republic of China] laws would not be applied in Hong Kong, the Standing Committee of the National People's Congress is empowered to designate specific [People's Republic of China] laws that may be applied in Hong Kong." Executive Branch PLCN Recommendation at 27 (citing *id.*, Exh. 125 at EB-PUBLIC-2176, Hong Kong Basic Law, Article 18); *see id.* at 28 (stating, "[o]fficially, the 'power of interpretation' of the Hong Kong Basic Law is 'vested in the Standing Committee of the National People's Congress.'") (citing *id.*, Exh. 125 at EB-PUBLIC-2219, Hong Kong Basic Law, Article 158); *see also* CUA Response to *Institution Order* at 23-24, n.104 (arguing, "[t]he [People's Republic of China] laws, except specifically listed on Annex III of the Basic Law, are not applicable in Hong Kong," and "[n]one of the laws and regulations quoted by the Commission or NTIA are included in Annex III").

entities; it treats them as 'branches' that focus on sales and customer service and controls them through the Hong Kong entity that directly owns CUA and all [CU's] overseas subsidiaries, [CUG]."[318]

69. Further, as the Commission stated in the *Institution Order*, the Commission has rejected arguments that Chinese law does not have extraterritorial effect.[319] CUA has offered no persuasive argument to dispel the significant concerns raised in the *Institution Order* that "[b]ased on the evidence before us and our assessment of [CUA's] relationship with its direct and indirect parent entities, as well as Chinese law, it appears that [CUA] is highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight."[320]

70. We accord deference to "'the Executive Branch's legal conclusion that China's National Intelligence Law and Cybersecurity Law, in particular, impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for Chinese intelligence-gathering activities.'"[321] We are not persuaded by CUA's arguments that the 2017 National Intelligence Law does not apply to CUA but "applies only to

[318] Executive Branch Response at 21; *see id.* at 21-22 (quoting from CU's 2018 Social Responsibility Report at 13, "'[CU] has been implementing the 'Belt & Road' ('B&R') initiative in depth. Relying on [CUG] and holding a vision of being a "customer-trusted international information service expert", the Company is committed to providing customers with highly safe, fast responding, excellent end-to-end experience, flexible, customized and concierge-like communications and information services. We have set up over 30 *branches* around the world to provide domestically and internationally integrated, global end-to-end comprehensive package information services to global customers and global voice and data services to individual customers abroad' (*emphasis added*)."). CUA contends that this "is an isolated statement by [CU] referring to some foreign operations as 'branches,'" that "[d]escribing a subsidiary as a 'branch' would be far short of ignoring its separate existence so as to warrant veil-piercing," and that CU's report "mentions both 'branch companies' and 'subsidiaries.'" CUA Reply to Executive Branch Letter at 13. As discussed above, we reject CUA's argument that the Commission is "piercing CUA's corporate veil . . . ." *See supra* para. 59; CUA Response to *Institution Order* at 39-40. The record reflects that serious national security and law enforcement concerns are associated with the ability of CUA's parent entities and ultimately the Chinese government to exercise significant and substantial influence and control over their subsidiaries, including CUA. Moreover, CUA has failed to refute these concerns while contending that "CUA is incorporated in the U.S., does not conduct any network business in the [People's Republic of China], and, therefore, is not governed by the Cybersecurity Law." CUA Response to *Institution Order* at 23.

[319] *Institution Order*, 36 FCC Rcd at 6341, para. 34 (citing *Huawei Designation Order*, 35 FCC Rcd at 14441-42, paras. 18-20); *see Huawei Designation Order*, 35 FCC Rcd at 14441-42, para. 20 (rejecting such argument raised by Huawei Technologies Company "after considering 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").

[320] *Institution Order*, 36 FCC Rcd at 6342, para. 34. *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 on Revocation and Termination* at *23-24, paras. 63-64.

[321] *Institution Order*, 36 FCC Rcd at 6341-42, para. 34 (quoting *Huawei Designation Order*, 35 FCC Rcd at 14441, para. 18); *see* Executive Branch Letter at 27-28 ("The 2017 Cybersecurity Law and the 2017 National Intelligence Law, in particular, impose affirmative legal responsibilities on Chinese and foreign citizens, companies, and organizations operating in China to provide access, cooperation, and support for Beijing's intelligence gathering activities."). As noted in the *Institution Order*, in the *Huawei Designation Order*, the Commission "accorded deference to the Executive Branch's 'risk-based interpretation of Chinese intelligence law' in keeping with Commission precedent." *Institution Order*, 36 FCC Rcd at 6342, n.143 (quoting *Huawei Designation Order*, 35 FCC Rcd at 14441, para. 19).

Chinese citizens and organizations."[322] We agree with the Office of the Secretary of Defense's assessment that "[t]he 2017 *National Intelligence Law* requires Chinese companies . . . to support, provide assistance, and cooperate in China's national intelligence work, *wherever they operate*."[323] The 2017 National Intelligence Law raises concerns about CUA's vulnerability to exploitation, influence, and control by the Chinese government, which CUA fails to refute. CUA has provided no persuasive argument to refute the significant concerns raised by the record that the Chinese government could require CUA to take certain actions in furtherance of China's national intelligence goals through the Chinese government's ownership and control of CUA's direct and indirect parent entities, and therefore, CUA.[324]

71. With respect to the 2019 Cryptography Law, we are unpersuaded by CUA's suggestion that this law cannot reach CUA. Article 26 of the Cryptography Law requires "any '[c]ommercial cryptography products that involve national security, the national welfare and the people's livelihood, or the societal public interest' to be tested and certified by Chinese government authorities, pursuant to the relevant provisions of the 2017 Cybersecurity Law."[325] As former Deputy Assistant Attorney General of

---

[322] CUA Response to *Institution Order* at 24. *See, e.g.*, Executive Branch Letter at 27-30 (discussing the consequences of the 2017 National Intelligence Law and other Chinese laws and addressing, for instance, Articles 7, 14, and 17 of the National Intelligence Law); *Institution Order*, 36 FCC Rcd at 6340-41, paras. 31-32. As we similarly stated in the *China Telecom Americas Order on Revocation and Termination*, "Article 7 of the 2017 National Intelligence Law states, '[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of. The State protects individuals and organizations that support, assist, and cooperate with national intelligence efforts.'" *China Telecom Americas Order on Revocation and Termination* at *23, para. 63 (quoting Executive Branch CTA Recommendation, Exh. 118 at EB-2738, China Law Translate, National Intelligence Law of the P.R.C. (2017)). We have also considered the former U.S. National Security Advisor's statement that under Article 7 of China's National Intelligence Law, "all Chinese companies must collaborate in gathering intelligence." *Id.* (quoting *China Telecom Americas Institution Order*, 35 FCC Rcd at 15018, para. 22 (citing H.R. McMaster, What China Wants, The Atlantic, May 2020, at 70, 71, 72-73)). While CUA suggests that the 2017 National Intelligence Law does not apply to CUA directly, CUA offers no argument or evidence that the law does not apply to its parent entities, or that it will not be subject to any request or directive from the Chinese government pursuant to such law, including through its the influence and control of its parent entities, or that it would be able to challenge or act independently of any such request or directive related to the Chinese government.

[323] Executive Branch Letter at 22, n.131 (quoting Office of the Sec'y of Def. Ann. Rep. to Cong., *Military and Security Developments Involving the People's Republic of China 2019*, at 101) (second emphasis added); *see id.* at 27-30; *see China Telecom Americas Order on Revocation and Termination* at *23, para. 63 (quoting Executive Branch CTA Recommendation at 35 & n.123 (citing *id.*, Exh. 115 at EB-2524, Office of the Secretary of Defense Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019 at 101 (May 2, 2019))) (emphasis added). *See also Applicability of National Intelligence Law to Chinese and non-Chinese Entities*, *supra* note 293 (stating that "[e]ntities established outside of China and which are owned by non-Chinese companies should in principle not be subject to [the National Intelligence Law]. . . . However, based on the wording of [the National Intelligence Law], Chinese citizens working for companies outside of China would technically be subject to [the law]. Many times, however, complying with [the National Intelligence Law] by cooperating with the Chinese intelligence services could result in breaches of local laws. . . . Chinese overseas subsidiaries, with Chinese headquarters, i.e. controlled by a parent company established in China, could be subject to [the National Intelligence Law] or made to comply with [the law][.]").

[324] As we stated above, CUA has provided no persuasive arguments against the Chinese government's influence and control of CUA through, for example, CUA's ties with the Chinese Communist Party, or that the Chinese government could also directly influence CUA to take certain actions. *See supra* paras. 51-63.

[325] Statement of Deputy Assistant Attorney General Adam S. Hickey at 7 (citing Economics and Trade Bulletin (U.S.-China Econ. And Sec. Review Comm'n) Nov. 5, 2019, at 13, https://www.uscc.gov/sites/default/files/2019-11/November%202019%20Trade%20Bulletin.pdf; China Law Translate, Cryptography Law of the P.R.C. (2019), https://www.chinalawtranslate.com/en/cryptography-law/ (accessed Feb. 20, 2020)). Deputy Assistant Attorney General Hickey stated that provisions contained in the 2019 Cryptography Law "impose requirements that will

(continued….)

the National Security Division, Adam Hickey, noted, "[n]one of these laws provide much, if any, detail about legal procedures or judicial oversight available to challenge Chinese government demands."[326] And again, CUA has proffered no persuasive evidence to refute the concerns raised by the record that the Chinese government could require CUA to take certain actions pursuant to these laws through the Chinese government's ownership and control of CUA's direct and indirect parent entities, and subsequently, CUA.

72. CUA claims that, "assuming, *arguendo*, that any of these three laws did apply to CUA, and that such laws allowed the Chinese government to request companies to assist Chinese intelligence efforts, the Commission has offered no evidence whatsoever that CUA has received, let alone complied with, any such requests from the Chinese government."[327] CUA argues that "the Commission once again resorts solely to speculative prognostications of what could happen" and that the Commission has not "provided examples of companies similarly situated to CUA that have been 'forced to comply' with such laws."[328] We find, however, that there are significant national security and law enforcement risks associated with CUA, the role in its management and operations by CUG, and its vulnerability to the influence and control of the Chinese government and Chinese Communist Party. We defer to the Executive Branch agencies' expertise in identifying and mitigating these risks, and ultimately reach an independent conclusion that the record evidence demonstrates that CUA's retention of its section 214 authority raises substantial national security and law enforcement risks because of these identified laws and CUA's relationship with its direct and indirect parent entities, and, for this and the reasons described below, that revocation is both appropriate and necessary in this case.[329]

b. CUA's Argument Concerning the Commission's "Foreign Policy Based" Approach in this Case is Unfounded

73. Finally, CUA observes that the Commission's "foreign policy based approach need not be limited to carriers with indirect relationships with the Chinese government" and cautions that "[i]f generalized foreign policy concerns suffice to revoke a section 214 authorization, then, in the future, the Commission may revoke the authorizations of carriers with connections to countries other than China; carriers controlled by private citizens from disfavored countries; or even carriers controlled by American citizens just because they provide service to a disfavored country or are somehow perceived to be a potential security risk."[330] CUA contends that "there would be little if any incentive for carriers to invest

(Continued from previous page)
expose commercial encryption used within China to testing and certification by the Chinese government, potentially facilitating" Chinese intelligence gathering activities. *Id*. at 6. *See* The National People's Congress of the People's Republic of China, Cryptography Law of the People's Republic of China (Passed Oct. 26, 2019, Effective Jan. 1, 2020), http://www npc.gov.cn/npc/c30834/201910/6f7be7dd5ae5459a8de8baf36296bc74.shtml.

[326] Statement of Deputy Assistant Attorney General Adam S. Hickey at 7 (discussing the 2017 Cybersecurity Law, 2017 National Intelligence Law, and 2019 Cryptography Law). Deputy Assistant Attorney General Hickey continues, "These laws are not merely defensive in nature: they enable the Chinese government to make affirmative demands on its people and entities to advance the Communist Party's interest." *Id*.

[327] CUA Response to *Institution Order* at 25.

[328] *Id*.

[329] We note that CUA argues that its "section 214 authorizations were lawfully obtained through the procedures and requirements promulgated by the Commission" and that the "Executive Branch agencies have not presented any evidence that CUA has followed any illegal instructions from CUG or the [People's Republic of China] government that would eviscerate the integrity of the Act." *Id*. at 39. Our actions herein are based on our public interest analysis that considers, among other things, the changed national security environment since CUA's section 214 authorizations were originally granted and the national security and law enforcement risks identified in the record. *See supra* paras. 27-28.

[330] CUA Response to *Institution Order* at 26.

in developing and maintaining facilities for international communications under these conditions, an outcome clearly contrary to the public interest," because "no carrier could have a legitimate expectation that a record of compliance would ensure the continued validity of its section 214 authorization if such authority could be revoked based on speculative possibilities."[331] We disagree. Prior to receipt of their authorizations, section 214 authorization holders are on notice that the Commission has the authority to revoke their section 214 authorizations based on the Commission's consideration of the public interest.[332] Further, CUA's argument ignores the significant national security and law enforcement risks specifically associated with Chinese government ownership and control of state-owned entities and their foreign subsidiaries, which have been widely recognized throughout the U.S. government.[333] Additionally, CUA has not offered any evidence to support its contention. Accordingly, we do not agree that our decision to revoke CUA's section 214 authority would disincentivize carriers to invest in international communications facilities in the United States.

2. CUA's Retention of Section 214 Authority Presents National Security and Law Enforcement Risks

74. Given the changed national security environment since the Commission authorized CUA to provide telecommunications services in the United States, and based on our review of the full record in this proceeding, we conclude that there are significant national security and law enforcement risks associated with CUA's retention of its section 214 authority that pose a clear and imminent threat to the security of the United States. As explained below, CUA's operations in the United States pursuant to its domestic and international section 214 authority, combined with those operations that do not require section 214 authority, provide CUA with access to U.S. telecommunications infrastructure and sensitive U.S. customer information. As the Executive Branch agencies point out, CUA's service offerings in the United States, including those made possible by its section 214 authority, "furnish CUA with access to more customers, communications traffic, and interconnections with other U.S. common carriers than it would have otherwise."[334] As discussed below, this access presents CUA, its controlling parent entities, and therefore the Chinese government, with numerous opportunities to access, monitor, store, disrupt, and/or misroute U.S. communications in ways that are not authorized and that can facilitate espionage and other activities harmful to U.S. national security and law enforcement interests. Because the Chinese government has influence and control over CUA, as discussed above, the record raises serious and unacceptable concerns that the Chinese government can, for example, direct or otherwise influence CUA to act on opportunities presented by its access to U.S. telecommunications infrastructure and U.S. customer information.[335] Despite being afforded several opportunities to address these national security and law enforcement risks, CUA failed to persuasively dispute or explain how they can be ameliorated.[336] Indeed, CUA did not address with particularity or otherwise respond to the national security and law enforcement concerns that we raised in the *Institution Order*.[337] Accordingly, we conclude that CUA's retention of section 214 authority presents national security and law enforcement risks that warrant revocation of its section 214 authority.

---

[331] *Id*.

[332] *See infra* para. 74.

[333] *See infra* para. 76.

[334] Executive Branch Letter at 34.

[335] *See supra* Section III.B.1; *see also* Executive Branch CTA Recommendation at 34 ("Like the applicant in [the *China Mobile USA Order*, China Telecom Americas], is indirectly majority-owned and controlled by the [Chinese] government and is vulnerable to exploitation, influence and control by the Chinese government.").

[336] *See supra* Section III.A.4.

[337] *See generally* CUA Response to *Institution Order.*

75. CUA has blanket domestic section 214 authority and holds two international section 214 authorizations that were granted in 2002.[338] CUA states that with regard to domestic interstate telecommunications services, it "has provided, or currently provides, the following telecommunications services:" Dedicated Private Line Circuits, EPL, and MVNO services.[339] With regard to U.S.-international telecommunication services, CUA states that it "has provided, or currently provides," the following telecommunications services: IPLC, IEPL, and MVNO.[340] Based on its filings, CUA appears to currently offer the above services pursuant to its section 214 authority.[341] In addition, CUA states that it provides "'information' or other non-telecommunications services."[342] CUA is authorized to, at any time, provide any other domestic service under blanket section 214 authority,[343] and to provide "international basic switched, private line, data, television and business services" under section 214 of the Act and its implementing rules.[344] Significantly, this authority allows a carrier to continue to extend its existing network in the United States, install new equipment or upgrade existing equipment on its network, or request additional interconnections with the networks of other U.S. common carriers—all without seeking further Commission approvals.[345]

76. Circumstances have changed dramatically since 2002, when the Commission first authorized CUA to provide telecommunications services in the United States. The Executive Branch agencies also recognize that the national security environment and China's role as a threat have evolved since 2002, at which time "the Director of Central Intelligence, George Tenet, told the Senate Armed Services Committee that 'Usama Bin Ladin and the al-Qa'ida network were the most immediate and serious threat this country faced,'"[346] and "China's campaign of economic espionage, illicit acquisition of U.S. sensitive technology and sensitive data, and cyber-enabled espionage were not contemplated as

[338] *See supra* para. 6.

[339] CUA Response to *Institution Order* at 44; *see infra* para. 77. CUA adds that "[t]o the extent these telecommunications services are or were *domestic* interstate telecommunications services, provided by CUA on a *common carrier basis*, CUA provides or has provided them pursuant to its blanket domestic section 214 authorization." CUA Response to *Institution Order* at 44.

[340] CUA Response to *Institution Order* at 45-46; *see infra* para. 77. CUA adds that "[t]o the extent these telecommunications services were or are *U.S.-international* telecommunications services, provided by CUA on a *common carrier basis*, CUA has provided or currently provides them pursuant to its international section 214 authorizations." CUA Response to *Institution Order* at 46.

[341] *See supra* para. 9; CUA Response to *Institution Order* at 44-46.

[342] CUA Response to *Order to Show Cause* at 25.

[343] 47 CFR § 63.01.

[344] 47 U.S.C. § 214; 47 CFR §§ 63.22(d), 63.23(c); 63.18(e)(1)-(2).

[345] 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).

[346] Executive Branch Letter at 2-3 (quoting *Worldwide Threat – Converging Dangers in a Post 9/11 World: Before the S. Select Comm. on Intelligence*, 107th Cong. (Feb. 6, 2002) (testimony of George J. Tenet, Director of Central Intelligence), https://avalon.law.yale.edu/sept11/tenet_002.asp); *see Institution Order*, 36 FCC Rcd at 6346, para. 40.

imminent or serious threats."[347] The Executive Branch agencies contend that the current threats facing the United States are different than those of 20 years ago, with cyber issues at the fore of the Office of the Director of National Intelligence's (ODNI) Worldwide Threat Assessment, and "with China being the first country identified by name for its persistent economic espionage and growing threat to core military and critical infrastructure systems."[348] ODNI's 2021 annual threat assessment observed that "China will remain the top threat to US technological competitiveness" and that the Chinese government employs "a variety of tools, from public investment to espionage and theft, to advance its technological capabilities."[349] ODNI continues to find that "China presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat."[350] Additionally, in recent years, the U.S. government has issued numerous official statements, testimonies, reports, and criminal indictments that highlight the significantly enhanced national security threat associated with the Chinese government's activities. For instance, the Executive Branch agencies state that according to DOJ charging documents, "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."[351] Similarly, the Director of the Federal Bureau of Investigation has warned that "no country poses a broader, more severe intelligence collection threat than China,"[352] while the Office of the U.S. Trade Representative (USTR) observed in its 2018 Section 301 Report that "cyber theft [was] one of China's preferred methods of collecting commercial information because of its . . . plausible deniability."[353] USTR's 2021 Section 301 Report notes that China remains on its Priority Watch List and is one of only

[347] Executive Branch Letter at 3; *see Institution Order*, 36 FCC Rcd at 6346, para. 40.

[348] Executive Branch Letter at 3 (citing 2019 Worldwide Threat Assessment by the Director of National Intelligence at 5); *see Institution Order*, 36 FCC Rcd at 6346, para. 40. The Executive Branch agencies cite to instances in which U.S. government agencies have detailed the security threats posed by the Chinese government. Executive Branch Letter at 3-6; *see, e.g.*, 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 (July 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. 1 (Dec. 12, 2018) (statement of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security), https://go.usa.gov/xss7f; 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/xtUqq; 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/xtUqa.

[349] Office of the Director of National Intelligence, *Annual Threat Assessment of the US Intelligence Community* at 7 (April 9, 2021), https://go.usa.gov/x6M7g.

[350] *Id.* at 8. Among other threats, ODNI's 2021 assessment observes that "China's cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US homeland . . . ." *Id.*

[351] Executive Branch Letter at 5; *see Institution Order*, 36 FCC Rcd at 6346, para. 40 & n.175. The Executive Branch agencies also cite to incidents of public law enforcement actions against Chinese actors. Executive Branch Letter at 5.

[352] 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/xeAqq.

[353] 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/xeAqC.

nine countries in the world so designated.[354] As we stated in the *Institution Order*, "[t]he Executive Branch agencies contend that, '[p]ut simply, the [Chinese] government uses its firms and companies as extensions of its apparatus. Those concerns are particularly acute with respect to [Chinese] state-owned enterprises ('SOEs') and their subsidiaries, because the [Chinese] government is able to exercise direct control over those entities.'"[355]

a. CUA's Section 214 Operations Provide it Enhanced Opportunity and Ability to Access, Monitor, Store, Disrupt, and/or Misroute U.S. Communications

77. Based on the totality of the evidence in the record, we find that the variety of services offered by CUA pursuant to its section 214 authority, as well as those not authorized pursuant to section 214 authority, provide CUA with access to U.S. telecommunications infrastructure and U.S. customer records. This access presents CUA, its controlling parent entities, and therefore, the Chinese government, with opportunities to access, monitor, store, disrupt, and/or misroute U.S. communications, and the opportunity to facilitate espionage and other activities harmful to the interests of the United States.[356] CUA identifies certain telecommunications services that it "has provided, or currently provides," under section 214 authority: MVNO, IPLC, International Wholesale Voice, and IEPL services.[357] CUA also states that it "has provided, or currently provides," domestic "Dedicated Private Line circuits" and domestic EPL under section 214 authority.[358] Based on CUA's responses and its marketing of services on its website, we understand that the domestic "Dedicated Private Line circuits" and domestic EPL are the domestic version of IPLC and IEPL services.[359] Any discussion of risks associated with IPLC and IEPL

---

[354] 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 5 (Apr. 2021), https://go.usa.gov/xeFMN. The Report notes that, "[s]ince enacting its Cybersecurity Law in 2017, China has continued to build on its policies for 'secure and controllable' Information Communications Technology (ICT) products, such as the issuance of the Cybersecurity Classified Protection Scheme in May 2020. Along with the adoption of the Cryptography Law in 2019 and the Cybersecurity Review Measures in 2020, these developments represent multiple steps backward through China's efforts to invoke cybersecurity as a pretext to force U.S. IP-intensive industries to disclose sensitive IP to the government, transfer it to a Chinese entity, or restrict market access." *Id*. at 48.

[355] *Institution Order*, 36 FCC Rcd at 6346, para. 40 (quoting Executive Branch Letter at 6). We also give weight to the Executive Branch agencies' statement that U.S. government warnings concerning the threats posed by Chinese government-sponsored cyber actors "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." Executive Branch Letter at 31; *Institution Order*, 36 FCC Rcd at 6347, n.177.

[356] Executive Branch Letter at 31-36.

[357] CUA Response to *Institution Order* at 44-46; *see supra* paras. 9, 75. As noted above, CUA asserts that it terminated its International Wholesale Voice offering in 2017. *See supra* para. 9; CUA Response to *Institution Order* at 46.

[358] CUA Response to *Institution Order* at 44; *see supra* paras. 9, 75. With regard to its domestic "telecommunications services," CUA states that it "resell[s] local partners' services to our end user customers": (1) "Dedicated Private Line circuits: a circuit that provides a dedicated, point-to-point circuit connection between two locations" and (2) "Ethernet Private Line: a service that provides dedicated point-to-point or point-to-multiple points Ethernet connections." CUA Response to *Institution Order* at 44.

[359] CUA's website advertises MVNO, IPLC, and IEPL services, but CUA does not advertise domestic Dedicated Private Line circuit service or domestic EPL service. China Unicom Americas, *IEPL*, https://unicomus.com/iepl/ (last visited Jan. 26, 2022); China Unicom Americas, *IPLC*, https://unicomus.com/iplc/ (last visited Jan. 26, 2022); *see* CUA Response to *Institution Order* at 44-46; CUA Response to *Order to Show Cause* at 23-25. From an engineering and technical perspective, the Dedicated Private Line circuit service and the EPL service would be the services provided domestically. *See e.g.,* World Trade Organization, Telecommunications Services, Glossary of Terms, https://www.wto.org/english/tratop_e/serv_e/telecom_e/tel12_e.htm (last visited Jan. 26, 2022) (defining

(continued….)

services includes the risks associated with the provision of domestic "Dedicated Private Line circuits" and domestic EPL.[360] CUA's provision of these domestic section 214 services provides it with an equivalent opportunity for CUA to access, monitor, store, disrupt, and/or misroute U.S. communications. We also recognize that CUA's ability to combine its section 214 services and those services that do not require section 214 authority, makes CUA more attractive as a service provider to U.S. customers than if it did not offer such a suite of services.[361] As the Executive Branch agencies observe, "CUA has provided a full suite of communications services and has steadily expanded its presence inside the United States since 2002."[362] This, in turn, increases the prospective U.S. customer base for CUA's section 214 services that are operated through CUA's Points of Presence (PoP) located within the United States.[363] The full suite of services offered by CUA, facilitated by CUA's physical presence in the United States, creates significant opportunity for CUA to conduct activities that are harmful to the national security and law enforcement interests of the United States.

78. The *Institution Order* provided a robust description of the Executive Branch agencies' statements concerning the ways in which "[CUA's] U.S. operations provide opportunities for [Chinese] government-sponsored actors to engage in espionage, theft of trade secrets and other confidential business information, and to collect, disrupt, or misroute U.S. communications."[364] Importantly, the Executive Branch agencies state that CUA, "as an international Section 214 authorization holder, is connected to the

(Continued from previous page)
"Private Leased Circuit Service" as "[t]he service of providing permanent transmission connection between two customer premises for the exclusive use by a customer. This service may be provided over facilities owned or operated by an operator or over transmission capacity sold or leased by a non-facilities-based telecommunications provider, or reseller, and may use terrestrial or satellite facilities. It generally does not involve central office switching operations. Also called a private leased line.").

[360] *See infra* paras. 91-110 (discussing IPLC and IEPL and the risks relevant to these and other services).

[361] CUA claims that certain of its services are currently provided on a common carrier basis, "[t]o the extent" they are telecommunications services, and that "it believes" that it can "continue to provide" all of its non-MVNO services "on a private carriage basis, without a section 214 authorization." CUA Response to *Institution Order* at 46. The classification of services as common or private carriage is a fact-based inquiry, governed by longstanding precedents. *See, e.g., National Ass'n of Regulatory Util. Comm'rs v. FCC,* 525 F.2d 830 (D.C. Cir. 1976); *Orloff v. FCC,* 352 F.3d 415 (D.C. Cir. 2003). We note that section 214 applies to the offering of telecommunications for a fee to the public at large or to such "classes of users" as to be effectively available to the public, 47 U.S.C. § 153(53), and that under such precedents minor differences in price or other terms of service do not alone qualify a service as private rather than common carrier in nature. CUA fails to provide the detailed and verifiable factual support needed for the Commission to evaluate its claim that other services besides MVNO are provided pursuant to individually tailored and negotiated contracts. We therefore base our findings on CUA's responses on the services CUA "has provided, or currently provides," and/or may provide in the future pursuant to section 214 authority, and the risks of combining section 214 services with non-section 214 services as a suite of services. *See infra* para. 110.

[362] Executive Branch Letter at 11.

[363] *See* PSI Report at 81 (stating that "CUA has established 11 points of presence—five on the East coast, five on the West coast, and one in the Midwest"); *see* China Unicom Global Limited, *Network Capabilities—PoPs*, https://network.chinaunicomglobal.com/#/district/north-america (last visited Jan. 26, 2022) (China Unicom Global PoPs) (presenting 10 locations in the United States, and corresponding weblinks, identified as "China Unicom Global PoPs"); *see infra* note 468. According to the PSI Report, CUA's 11 points of presence "are located in (1) Seattle, WA; (2) Hillsboro, OR; (3) Palo Alto, CA; (4) San Jose, CA; (5) Los Angeles, CA; (6) Dallas, TX; (7) Reston, VA; (8) Ashburn, VA; (9) Chicago, IL; (10) New York, NY; and (11) Miami, FL." *Id.* at n.498 (citing Briefing with China Unicom Americas (Apr. 16, 2020)). {[

]} *See* CUA Response to *Institution Order*, Business Confidential Exh. 5 at 1-2 ({[ ]}). With regard to CUA's services such as IPLC and IEPL services, those services use the PoPs, routers, servers, and related infrastructure of CUA and its peering partners. *See infra* para. 97 (discussing CUA's peering partners).

[364] *Institution Order*, 36 FCC Rcd at 6347, para. 41 (quoting Executive Branch Letter at 31).

domestic telecommunications networks of the United States and has direct access to the telephone lines, fiber-optic cables, cellular networks, and communication satellites that constitute those networks," and that "[s]uch connections and access can provide a strategic capability to target, collect, alter, block, and re-route network traffic."[365] The Executive Branch agencies add that "the [Chinese] government could use CUA's status as a common carrier '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,' and that the Chinese government 'would have greater ability to monitor, degrade, and disrupt U.S. government communications' through [CUA]."[366] In the *Institution Order*, we recognized the Executive Branch agencies' statement that because China's Internet network is largely isolated, CUA's PoPs in North America are vital to provide China with "a strategic advantage in that the 'imbalance in access allows for malicious behavior by China through [Chinese telecommunication carriers] at a time and place of its choosing, while denying the same to the US and its allies.'"[367] The *Institution Order* also included our independent concern, as the expert agency with respect to communications technology, that CUA, "like other similarly situated providers of MVNO service, may be able to use BGP routing to forward to China interconnected VoIP traffic without the knowledge or authorization of the customer, and for purposes that may include espionage or threats to U.S. national security."[368] Ultimately, based on the record evidence, our concerns remain that CUA is vulnerable to exploitation, influence, and control by the Chinese government through its parent entities, and that "[t]his vulnerability presents opportunities for the Chinese government to conduct various activities that would ultimately pose significant threats to U.S. national security and law enforcement interests."[369]

79. As discussed below, the opportunities for harmful conduct exist in at least two broad categories. First, as a provider of MVNO service, CUA has the opportunity to access CPNI, call detail

---

[365] Executive Branch Letter at 31; *see Institution Order*, 36 FCC Rcd at 6347, para. 41.

[366] Executive Branch Letter at 31. *See Institution Order*, 36 FCC Rcd at 6347, para. 41. In the *Institution Order*, the Commission expressed concern with "the fact that [CUA] informed the Senate Subcommittee that [CUG]—which, according to the record, is subject to Chinese laws—monitors [CUA's] network operations and can remotely configure [CUA's] network equipment." *Id.* & n.183 (citing PSI Report at 79).

[367] *Institution Order*, 36 FCC Rcd at 6347-48, para. 42; Executive Branch Letter at 34-35 (quoting Chris C. Demchak & Yuval Shavitt, *China's Maxim - Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking*, Military Cyber Affairs, Vol. 3 Iss. 1 at 8 (2018). According to the Executive Branch agencies, CUA "has 11 Points of Presence in the United States and operates an unknown number of [BGP] routers, and advertises BGP routing information to peering partners, which include 'major Tier 1 Internet service providers such as Level 3, Verizon, and Cogent.'" *Institution Order*, 36 FCC Rcd at 6348, para. 42; Executive Branch Letter at 35; *see* PSI Report at 81; AS19174 China Unicom (Americas) Operations Ltd, https://bgp he net/AS19174 (last visited Jan. 26, 2022).

[368] *Institution Order*, 36 FCC Rcd at 6348, para. 42 (citing 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). The Commission noted that CUA, "for example, could maliciously or accidentally redirect to China VoIP data traffic from an MNO or MVNO by mounting a BGP route attack originated at or through one of its 11 Points of Presence, for example, from [CUA's] BGP routers, a scenario enabled by [CUA] using BGP as is customary with its peering partners." *Id.* (citing Catalin Cimpanu, *China has been "hijacking the vital internet backbone of western countries*," ZDNet (Oct. 26, 2018), https://www.zdnet.com/article/china-has-been-hijacking-the-vital-internet-backbone-of-western-countries/).

[369] *Id*. Significantly, the Commission noted that "in an independent analysis of attacks initiated by foreign networks that targeted U.S. mobile users and devices, and that were detected by U.S. mobile operators' international Signaling System 7 (SS7) signaling links, a component of [CU] was identified as the likely source of more such attacks than any other provider in the world from May 2018 to December 2019." *Id.* (citing Exigent Media, *Far From Home: Active Foreign Surveillance of U.S. Mobile Users 2018-2019: Threat Intelligence Report*, 13, 16, https://img1.wsimg.com/blobby/go/cda61771-2b5c-4a41-aac5-0bd319d1fe07/downloads/Far-From-Home_Intel-RP_2018-2019_B.pdf?ver=1608567073472 (last visited Jan. 26, 2022)).

records (CDRs), and at least some personally identifiable information (PII). This opportunity for access to sensitive customer information exists, at least to some degree, regardless of whether CUA, in its role as an MVNO, {[ ]} In fact, the record evidence shows that CUA's records for its MVNO customers are made available to {[ ]}[370] Second, as a provider of section 214 services and various other services that allow it to carry U.S. communications traffic, CUA has the opportunity to access, monitor, store, disrupt, and/or misroute those communications in ways that provide unauthorized access to U.S. customer data and/or metadata.[371] CUA has the ability to cause its customer traffic to be routed through unexpected paths, such as a path with significant portions routed outside the United States, even if the origination and destination of the traffic are within the United States. Such routing might occur as a result of normal peering and routing policies that CUA may have in place with its ultimate parent, CU.[372] Traffic that is carried in this manner is potentially subject to path diversions that traverse one or more locations outside of the United States. These path diversions may decrease service performance to U.S. customers and—more importantly and relevant to our assessment here—may increase national security and law enforcement risks if the path travels, for example, from the United States, to China, and back to the United States.[373] Importantly, CUA's PoPs within the United States provide CUA with the opportunity to access, monitor, store, disrupt, and/or misroute traffic. The distinction between these two scenarios—the ability to access, monitor, store, disrupt and/or misroute traffic from within the United States as compared to outside of the United States—is that PoPs in the United States are subject to U.S. laws and regulations, while traffic routed through networks in other countries can be accessed, monitored, stored, disrupted and/or misrouted, potentially beyond the reach of U.S. laws or regulations that prohibit such actions. Significantly, CUA, its controlling parent entities, and the Chinese government can direct path diversions that can facilitate unauthorized access to the underlying communications. In addition to the diversion of traffic, the risks identified in the record further include the possibility of intentional misrouting of traffic by CUA through a process described below.[374]

---

[370] CUA Response to *Institution Order*, Business Confidential Exh. 3. {[ ]} *See supra* paras. 57-58. {[ ]} *See Institution Order*, 36 FCC Rcd at 6362, Appx. A.

[371] We note that metadata may be used for authorized purposes as part of a network service provider's normal course of operations. At a general level, "metadata" constitute information that describes or summarizes other information to make it useful. *See* Oxford Learner's Dictionary, https://www.oxfordlearnersdictionaries.com/us/definition/english/metadata?q=metadata (defining "metadata"). In the context of communications, "metadata" may include "a range of information, such as the source, destination and timing of a particular communication, but not its content." *See* Rohan Pearce, *Data retention: Law enforcement accessed 'metadata' more than 296k times in FY18*, ComputerWorld (July 23, 2019) https://www.computerworld.com/article/3472422/data-retention-law-enforcement-accessed-metadata-more-than-296k-times-in-fy18 html.

[372] *See infra* para. 97, notes 454, 483; *see supra* notes 368, 369.

[373] *See infra* paras. 97-99.

[374] Misrouting is the configuration of routing policies, or advertising of false routes (*e.g.*, BGP hijacking), to ensure that traffic is forwarded through locations from which bad actors can monitor and/or manipulate data using sub-

(continued….)

80. While we recognize that any service provider has the opportunity to engage in sub-optimal traffic path diversions or intentional misrouting, other such providers are not identified like CUA as posing a national security and law enforcement risk to the United States.[375] Based on the record in this proceeding as well as publicly available information, we assess that CUA's network operates in conjunction with that of its indirect controlling parent, CU, and thus CUA can utilize CU's infrastructure in China (or that of CU's subsidiaries in other countries) as part of the normal network operations associated with CUA's offering of section 214 services and other services.[376] Indeed, CUA describes its ability to leverage CU's network and infrastructure as an advantage in its company promotions.[377] Further, CUA is ultimately owned and controlled by the Chinese government. In light of the Chinese government's influence and control over CUA, we find that the opportunities for CUA, as well as its parent entities, to engage in espionage and other harmful activities through its operations in the United States present especially significant threats to the security of the U.S. telecommunications infrastructure, the information that is carried on this infrastructure, and the individuals and companies that use the services offered by CUA.

(i) MVNO Service

81. We find that there are significant national security and law enforcement risks associated with CUA's retention of its section 214 authority to provide MVNO services. As described below, we reject CUA's characterization of the extent to which it has access to sensitive customer information,[378] and we set out various means by which CUA can access this information and the threats presented by such access. We observe that, as an MVNO, CUA has the opportunity to collect a significant amount of U.S. customer information through CDRs.[379] We also assess that CUA has the opportunity to collect PII.

(Continued from previous page)
optimal routes (*i.e.*, routes that are not the shortest path, nor reflect a least cost path, between the origination and destination). *China Telecom Americas Order on Revocation and Termination* at *26, para. 70, n.319; *Institution Order*, 36 FCC Rcd at 6347, para. 41.

[375] *Institution Order*, 36 FCC Rcd at 6336-6353, paras. 27-48.

[376] *See infra* notes 428, 430. The PSI Report states that CUA "is China Unicom's American subsidiary and largest international affiliate." PSI Report at 74 (citing Briefing with China Unicom Americas, Apr. 16, 2020). Additionally, CUA's webpage titled "About Us" states that "[CUA] provides reliable and integrated end-to-end telecommunication services and solutions. We are the trusted partner of U.S.-based businesses seeking one-stop connectivity with China and beyond." *See* China Unicom Americas, *About Us*, https://unicomus.com/company-profile/ (last visited Jan. 26, 2022). CUA's webpage titled "IP Transits" states, "[o]ur Global IP Transit provides the service to content providers, medium or large enterprise customers who have their own AS numbers and IP addresses with Border Gateway Protocol (BGP) for various bandwidth accesses to AS10099 global network based in Hong Kong and covering overseas. With the service, internet contents in China can be released to the global Internet, overseas Internet users can access contents produced by enterprises and institutions located in mainland China with lower latency and higher access speed." China Unicom Americas, *IP Transits*, https://unicomus.com/ip-transits/ (China Unicom Americas, *IP Transits*) (last visited Jan. 26, 2022).

[377] *See, e.g.,* China Unicom Americas, https://unicomus.com/ (last visited Jan. 26, 2022) (*China Unicom Americas Website*); China Unicom Americas, Network Capabilities, North America, https://network.chinaunicomglobal.com/#/district/north-america (last visited Jan. 26, 2022).

[378] *See infra* paras. 83-86.

[379] *See* Florin Vancea, Codruta Vancea, Daniela Elena Popescu, Doina Zmaranda, and Gianina Gabor, "*Secure Data Retention of Call Detail Records*," Int'l J. of Computers, Comm. & Control: Vol. V, No. 5, at 961-967 (Dec. 2010), https://www researchgate.net/publication/228991607_Secure_Data_Retention_of_Call_Detail_Records (*Secure Data Retention of CDRs*). We note that CDRs are one example of CPNI, which includes numbers called and the frequency, duration, and timing of calls. *See* 47 U.S.C. § 222(h)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6931, para. 5. "CDR" is a term of art and was initially attributed to circuit switched voice traffic and the current
(continued….)

Further, CUA is able to {[ ]} without the authorization of its customers, which equates to a form of denial of service at the time and choosing of CUA.[380]

82. CUA describes its MVNO services as "mobile pre-paid services marketed to Chinese-speaking customers in the U.S., including visiting tourists."[381] CUA explains that these MVNO services "are provided by leasing network capacity from a U.S. domestic network operator, and include: local, interstate, and international voice, short message services ('SMS') and mobile Internet access services."[382] CUA operates its MVNO service under the brand name "CUniq," which is described by CUG as an "[MVNO] business in America."[383] As noted by the Executive Branch agencies, "[t]hrough CUA, [CUG] offers voice and data plans where voice and data is shared between phone numbers in the United States, China, and Hong Kong, which it enables by providing its users linked U.S., Chinese, and Hong Kong SIM cards."[384] Regarding CUA's management of its MVNO service, CUA explains that it {[ ]}[385] CUA clarifies that the services it provides as an MVNO that are not delegated to a

(Continued from previous page)
2021 3GPP specifications use the term "Charging Data Record." A CDR represents a "formatted collection of information about a chargeable event (e.g., time of call set-up, duration of the call, amount of data transferred, etc.) for use in billing and accounting." 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Charging management; Charging Data Record (CDR) parameter description (Release 16) (3GPP TS 32.298 V16.8.0) at 23 (Mar. 2021), https://www.3gpp.org/ftp/Specs/archive/32_series/32.298/32298-g80.zip (*3GPP – Charging Data Record*); 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service aspects; Charging and Billing at 5-6 (3G TS 22.105 version 3.2.0) at 5-6 (Oct. 1999), https://www.3gpp.org/ftp/Specs/archive/22_series/22.115/22115-320.pdf (*3GPP – Charging and Billing*) (defining "Call Detail Record (CDR)," "Charging," and "Billing"); *see ACLU v. Clapper,* 785 F.3d 787, 793 (2nd Cir. 2015) (defining "telephone metadata"); *Rural Call Completion,* WC Docket 13-39, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 16154, 16174-75, para. 42 (2013) (discussing CDRs); Alliance for Telecommunications Industry Solutions (ATIS), *call detail recording*, ATIS Telecom Glossary, https://glossary.atis.org/glossary/call-detail-recording-cdr/?search=call%20detail%20recording&page_number=&sort=ASC.

[380] *See* CUA Response to *Institution Order*, Business Confidential Exh. 5 at 2 ({[ ]}). *See also*, China Unicom, User Manual (V.9), https://www.mychinaunicom.com/file/User%20Manual%20(V.9).pdf (China Unicom User Manual) (last accessed Jan. 26, 2022). This user manual includes regulations and conditions for use of "China Unicom" SIM cards, with conditions under which mobile service will be deactivated. This same manual includes a "Notice of Telecom and Internet fraud crime legal liability," by the Ministry of Industry and Information Technology, which references the Network Security Law of the People's Republic of China, the Antiterrorism Law of the People's Republic of China, and other laws, and includes a declaration of compliance to be hand-written and signed by the user. China Unicom User Manual at 16-17.

[381] CUA Response to *Institution Order* at 44.

[382] *Id*.

[383] China Unicom Global Limited, *China Unicom Global Launches "CUniq" MVNO Business in America* (Mar. 4, 2017), https://www.prnewswire.com/news-releases/china-unicom-global-launches-cuniq-mvno-business-in-america-300418091.html ("On March 3, 2017, China Unicom Global Limited ("CUG") launched "CUniq" mobile virtual network operator ("MVNO") business in America . . . ."); *see also* CUniq, https://www.cuniq.com/us/plans/share-plan.html (CUniq) (last visited Jan. 26, 2022).

[384] Executive Branch Letter at 33 (citing CUniq, *supra* note 383).

[385] CUA Response to *Institution Order*, Business Confidential Exh. 5 at 1.

third party include {[

]}[386]

83. The Commission expressed concern in the *Institution Order* that CUA's service offerings provide CUA with access to both customer PII and CPNI, and that "this access presents risks related to the protection of sensitive customer information and the effectiveness of U.S. law enforcement efforts."[387] In the *Institution Order*, the Commission stated that CUA's provision of MVNO, IPLC, and IEPL services would likely provide CUA with 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."[388] In addition, the Commission observed that CUA likely also has "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."[389] The Commission noted that "usage information could be combined with a customer's PII to provide significant details to [CUA] and its parent entities, potentially providing opportunities for Chinese government-sponsored actors to engage in information collection activities or espionage of U.S. targets, or for any other activities that are contrary to the protection of U.S. customer records and U.S. interests."[390] The Commission added that CUA is required to be capable of complying with legal requests for information issued by the U.S. government pursuant to the Communications Assistance for Law Enforcement Act (CALEA),[391] and CUA would have knowledge of U.S. government requests concerning electronic surveillance for which CUA's assistance is requested, as well as knowledge of government requests for access to customer records.[392]

---

[386] *Id.*, Business Confidential Exh. 5 at 2.

[387] *Institution Order*, 36 FCC Rcd at 6352, para. 48.

[388] *Id*. (citing *TerraCom, Inc. and YourTel America, Inc.*, Notice of Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13331, para. 17 (2014) ("[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")).

[389] *Id.*; *see id*. at n.216 ("*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 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)).").

[390] *Id*. at 6352, para. 48.

[391] *Id*. at 6352-53, para. 48; *see id.* at n.218 (citing "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'").

[392] *Id*. at 6352-53, para. 48.

84. In its response to the *Institution Order*, CUA does not dispute that it has access to CPNI but adds that "it does not collect PII such as the customer's Social Security number, driver's license number, bank account number, or email address, but only uses the customer's name and phone number to contact and provide customer service."[393] CUA further states that it {[ ]}[394] In describing its management of customer information for both MVNO and enterprise customers, CUA clarifies that it {[ ]}[395] CUA also maintains that, as an MVNO, it "has implemented a CPNI protection policy to safeguard CPNI."[396]

85. Given the record evidence in this proceeding, we conclude that, as a provider of MVNO service, CUA has the opportunity to access CPNI, including CDRs, and that CUA may access at least some PII. This access provides opportunity to engage in activities that are harmful to the law enforcement and national security interests of the United States. CUA's access to CPNI is undisputed and we assess that the services CUA provides as an MVNO necessarily mean it has access to at least some degree of customer PII. Specifically, given that CUA provides, among other services, {[ ]},[397] we find it highly implausible that CUA does not have access to its customers' PII. We further find CUA's characterization of its practices—*e.g.*, that it "does not collect PII such as the customer's Social Security number, driver's license number, bank account number, or email address, but only uses the customer's name and phone number to contact and provide customer service"[398]—as indicative of CUA's lack of understanding of what PII is, or a lack of transparency in its response. Specifically, CUA's contention that it does not collect PII is inconsistent with {[ ]}[399]

86. We further conclude that, even if CUA does not request its customers' PII in the course of its normal business operations, like any similarly situated provider of MVNO service, CUA has direct access to sensitive U.S. customer information in CDRs.[400] The need to protect each CDR has long been

---

[393] CUA Response to *Institution Order* at 41.

[394] *Id.*, Business Confidential Exh. 3 at 1.

[395] *Id.*

[396] *Id.* at 41.

[397] *Id.*, Business Confidential Exh. 5 at 1-2.

[398] *Id.* at 41.

[399] *Id.*, Business Confidential Exh. 5 at 2. The Commission asked CUA to, "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," and that CUA provide "a description and copy of any policies and/or procedures in place to protect [PII and CPNI]." *See Institution Order*, 36 FCC Rcd at 6362-63, Appx A. As stated above, CUA's response was that it {[ ]} CUA Response to *Institution Order*, Business Confidential Exh. 3 at 1. We find this response incongruent.

[400] *See supra* para. 85.

recognized.[401] Even without revealing the content of communications, CDRs can reveal significant information.[402] For example, this information can include customer location in terms of the latitude/longitude of the cell tower used, both the calling number and called number, and the date, time, and duration of the call—all of which would be available to CUA.[403] This information can be valuable; according to media reports, a "massive-scale" espionage conducted over a period of seven years targeted and obtained CDRs (including times and dates of calls and cell-based locations) by breaking into more than ten mobile service providers' networks around the world,[404] including Africa, Asia, Europe, and the Middle East.[405] While service providers understandably focus their cybersecurity efforts on the need to protect their customers' CDRs from such hacking incidents,[406] the same potential for harm exists where service providers have access to customers' CDRs and thus opportunity to misuse this information. In contrast to hackers that would need to exert substantial effort to obtain access to CDRs and opportunity to misuse such information, an MVNO, such as CUA, has direct access to CDRs, which facilitates opportunity to access and misuse such information.

87. As we indicated in the *Institution Order*, CUA's management of customer records for its MVNO service, in particular the maintenance of such records outside of the United States and the access by non-CUA personnel, presents significant and unacceptable risks. Regarding the location of customer records, as noted in the PSI Report, CUA stated to the Senate Subcommittee that its customer records were stored on servers in Hong Kong and maintained by CUG.[407] Based on this, in the *Institution Order*, the Commission asked CUA to respond to the inconsistency. CUA's response to the *Institution Order* indicates that CUG manages U.S. customer records for CUA, and that U.S. customer records are {[

[401] Under U.S. law, CDRs are protected by such statutory provisions as 18 U.S.C. §§ 2701-2713, 3121-3127; 50 U.S.C. §§ 1801-1813, 1841-1846; 47 U.S.C. § 222. *See also Secure Data Retention of CDRs*, *supra* note 379.

[402] *ACLU v. Clapper*, 785 F.3d at 794 (reviewing "the startling amount of detailed information metadata can reveal—information that could traditionally only be obtained by examining the contents of communications 'and that is therefore often a proxy for content.' For example, a call to a single-purpose telephone number such as a 'hotline' might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships." (citations omitted)). *See* Zack Whittaker, *Hackers are stealing years of call records from hacked cell networks* (June 24, 2019), https://techcrunch.com/2019/06/24/hackers-cell-networks-call-records-theft/ (Whittaker).

[403] For an example of the information that an MNO could reasonably be expected to provide to its MVNO, *see* I.R.I.S. LLC, T-Mobile Metro PCS Interpreting Call Detail with Cell Site (Digger Reports) (updated Sept. 24, 2015), https://www.irisinvestigations.com/wp-content/uploads/2016/12/ToolBox/08-CALL%20DETAIL%20&%20CELL%20SITE/T-Mobile%20Metro%20PCS%20Interpreting%20CDR-Cell%20Site%20Reports.pdf.

[404] Whittaker, *supra* note 402; *see* Jon Porter, *Hackers steal call records from cell providers in 'massive-scale' espionage* (June 25, 2019), https://www.theverge.com/2019/6/25/18744020/operation-softcell-hack-call-detail-records-apt10-cybersecurity-cell-network-providers (Porter).

[405] *See* Porter, *supra* note 404.

[406] *See Secure Data Retention of CDRs*, *supra* note 379.

[407] PSI Report at 79.

[408] CUA Response to *Institution Order*, Business Confidential Exh. 3 at 1 ({

]}).

]}[410]

88. Regarding access to CUA's U.S. customer records by non-CUA personnel, both the Executive Branch agencies and the PSI Report note that for its MVNO service, CUA provides access to these records to CUA as well as CUG personnel.[411] The PSI Report further notes that CUG monitors CUA's U.S. network operations and has the ability to configure CUA's network equipment.[412] We observe that a {[

]}[413] This information contradicts CUA's statement in the record that it {[

]}[414] In addition, as the PSI Report observed, according to CUA, it uses a service platform based in Hong Kong for its MVNO service because "the subscriber base does not warrant a standalone U.S. platform."[415] CUA's responses to the Commission did not address this argument regarding the size of the subscriber base.

89. We disagree with CUA's assertions and conclude that a Hong Kong-based NOC that gathers data and metadata[416] on the U.S. customers of CUA, both through the maintenance of records and the management of the network, presents national security and law enforcement risks. Further, regardless of its location, the operation of this NOC by CUA's parent, CUG, raises especially significant national security and law enforcement concerns given the information that would be made available to CUG and its ultimate ownership by the Chinese government.

90. Accordingly, we find that, in its role as an MVNO, CUA's access to sensitive customer information poses serious risks to U.S. national security and law enforcement interests. We observe that the sensitivity of this information can be greatly enhanced and pose even greater risks when it is combined with other information that CUA can access from network communications and metadata.[417] We further conclude that the fact that CUA's MVNO service and related data involve CUA's parent entity, which is based in Hong Kong, {[

]} and whose parent entities are ultimately controlled by the Chinese government, raises significant national security and law enforcement concerns. Allowing CUA to continue to operate as an MVNO would be contrary to the national security and law enforcement interests of the United States.

---

[409] *Id*. at 1-2.

[410] *Id*.; *see infra* at Section III.B.3.

[411] Executive Branch Letter at 32; PSI Report at 79.

[412] PSI Report at 79.

[413] CUA Response to *Institution Order*, Business Confidential Exh. 3 at 3; *id*. (stating that {[

]}).

[414] *Id*., Business Confidential Exh. 3 at 1.

[415] PSI Report at 79.

[416] *See supra* note 371 (presenting definition and discussion of metadata).

[417] *Id*.

(ii) IPLC and IEPL Services Offered Under Section 214 Authority, and Other Network-Based Services

91. We find that IPLC and IEPL, which are offered pursuant to section 214 authority, and other network-based services provided by CUA, also offer substantial opportunities for CUA to access, monitor, store, disrupt, and/or misroute U.S. communications, and therefore present significant national security and law enforcement risks. As the Executive Branch agencies note, CUA has steadily expanded its presence inside the United States since receiving its international section 214 authorizations in 2002.[418] As explained below, CUA's expanded presence includes the establishment of physical operations through means such as co-location, as well as the provision of various services offered to retail, enterprise and other types of customers.

92. In addition to the MVNO service discussed above, CUA states that it provides IPLC[419] and IEPL services under section 214 authority.[420] CUA also indicates that it provides other services: MPLS VPN,[421] SVN,[422] IP Transit,[423] DIA,[424] IDC,[425] Cloud Computing,[426] and Resold Services.[427] CUA

[418] Executive Branch Letter at 11-17.

[419] *See supra* paras. 75, 77; CUA Response to *Order to Show Cause* at 23 ("International Private Leased Circuit ('IPLC') provides cross-border and cross-region customers with real-time transmission application designated for level-1 international data with the globally-covered Synchronous Digital Hierarchy (SDH) and Wavelength Division Multiplex (WDM) transmission network. The service is a fully transparent end-to-end private line service with a strict bandwidth guarantee and dedicated customer bandwidth."); CUA Response to *Institution Order* at 45.

[420] *See supra* paras. 75, 77; CUA Response to *Order to Show Cause* at 23 ("International Ethernet Private Line ('IEPL') provides customers with flexible bandwidth adjustment, from 2 Mbps to 10 Gbps, and Ethernet access capacity based on the multi-service transmission platform technology ("MSTP") relying on CUA's platform to access the global transmission network of CUG. It is a fully transparent point-to-point and point-to-multipoint private line service with strict bandwidth guarantee and dedicated customer bandwidth."); CUA Response to *Institution Order* at 45-46.

[421] CUA Response to *Order to Show Cause* at 23 ("Multi-protocol Label Switching Virtual Private Network ('MPLS VPN') services use MPLS to provide secure data communications such as internal data, audio, images, and videos between a customer's multiple locations. MPLS VPN services provide the customer with point-to-point and point-to-multipoint internal dedicated network communications.").

[422] *Id*. at 23 ("Smart Video Network ('SVN') services provide customers with IP-based, global video media services, including the real-time transmission, storage, and forwarding of audio, video, and other large media files.").

[423] *Id*. at 24 ("IP Transit services: AS4837/AS10099/AS19174 network platform is used to integrate with customers via a border gateway protocol (BGP) to provide global Internet penetration service for the customers' own IP address, as well as exclusive bandwidth to access content on the Internet."). According to the American Registry of Internet Numbers (ARIN), "[a]n Autonomous System (AS) is a group of one or more IP prefixes run by one or more network operators that maintains a single, clearly defined routing policy. An IP prefix is a list of IP addresses that can be reached from that ISP's network. The network operators must have an ASN to control routing within their networks and to exchange routing information with other ISPs." *Requesting IP Addresses or ASNs*, ARIN, https://www.arin net/resources/guide/request/. According to ARIN, CUA has been assigned the autonomous system number AS 19174. WHOIS-RWS, ARIN, https://whois.arin net/rest/org/CUAOL/asns. The other two AS numbers were assigned by APNIC to China Unicom networks. WHOIS-RWS, AS 19174, ARIN, https://whois.arin net/rest/asn/AS19174 ("Organization: China Unicom (Americas) Operations Ltd"); APNIC WHOIS Database, AS 4837, http://wq.apnic.net/apnic-bin/whois.pl?searchtext=AS4837:AS-CNCGROUP&form_type=advanced (AS4837 is maintained by "China Unicom Group Network"); APNIC WHOIS Database, AS 10099, https://wq.apnic.net/static/search html?query=as10099 (AS 10099, described as "China Unicom Global IP Servcies [sic]," maintained by "MAINT-HK-UNICOM," which is described as "China Unicom Global Limited").

[424] CUA Response to *Order to Show Cause* at 24 ("Dedicated Internet Access ('DIA') provides customers with various speeds of Internet access with guaranteed bandwidth, as well as access to CUA's Internet network".).

promotes these services as part of its service packages,[428] and it is able to combine these services, both those that require and those that do not require section 214 authority, in ways that make its service offerings more attractive and thereby present opportunities for CUA to engage in activities that undermine the security of the United States. CUA's online presence emphasizes the value it creates from these service packages as well as the global reach provided by its relationship with its ultimate parent, CU.[429] CUA's website describes this global reach, made possible by CU and its affiliated entities through CUG, as follows: "Our global network supports a wide portfolio of international voice and data solutions, cost-effective value-added services and a range of network monitoring services. With an extensive network infrastructure covering more than 30 countries and regions, we provide services for enterprise and carrier customers around the world."[430] CUA's provision of these services to customers in the United States, combined with its relationship to CU and its ultimate ownership by the Chinese government, presents significant national security and law enforcement risks. These risks exist because, in the course of providing its services, CUA can access, monitor, store, disrupt, and/or misroute U.S. communications without authorization, which in turn threatens the security and integrity of such communications.

93. As an initial matter, fundamental to protecting the security of the United States is the ability to trust that a service provider will uphold the confidentiality and integrity of information on the traffic that it stores or transmits. The risks of attacks on the confidentiality and integrity of information—or cybersecurity attacks—are greatest when bad actors have access to customer traffic through the routers, switches, and/or servers (i.e., the devices) that store or forward traffic through their network.[431] Bad

(Continued from previous page)

[425] *Id*. ("Data Center ('IDC') services provide customers with carrier-grade colocation space with high speed Internet access for the installation and operation of the customer's equipment. Services include physical colocation space, Internet access, electricity, and IP address leasing.").

[426] *Id.* ("Cloud Computing provides customers with a resold third-party cloud computing platform and application services, that includes virtual computing, data storage, and Internet access.").

[427] *Id*. (stating that CUA "also resells dark fiber, data center services, and system integration offered by its local partners ('Resold Services').."). CUA maintains that the "[t]elecommunications services offered by CUA include: MVNO, IPLC, and IEPL. The 'information' or non-telecommunications services offered by CUA include: MPLS VPN, IP Transit, SVN, DIA, IDC, Cloud Services, and the Resold Services." *Id*. at 24-25; *see also* CUA Response to *Institution Order* at 47.

[428] *See China Unicom Americas Website*, *supra* note 377 (identifying "Products and Services," including "Transmission," (IPLC, IEPL), "Global VPN" (MPLS VPN, IPsec VPN), "Internet" (IP Transits, Paid Peer, Global DIA, China DIA), and "Cloud & Managed Network Services" (Cloud Bond, SD-WAN) and noting that CUA "provides reliable and integrated end-to-end telecommunication services and solutions"; China Unicom Americas, *IP* Transits, *supra* note 376 ("Our Global IP Transit provides the service to content providers, medium or large enterprise customers who have their own AS numbers and IP addresses with [BGP] for various bandwidth accesses to AS10099 global network based in Hong Kong and covering overseas. With the service, internet contents in China can be released to the global Internet, overseas Internet users can access contents produced by enterprises and institutions located in mainland China with lower latency and higher access speed."); *see supra* note 423 (explaining that Autonomous System Number AS10099 is assigned to "China Unicom Global").

[429] *China Unicom Americas Website*, *supra* note 377.

[430] *See id*.; CUA Response to *Order to Show Cause*, Business Confidential Exh. 6 at 2 ({[

]}).

[431] *See* Federal Trade Commission, *A Look at What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers,* FTC Staff Report at i (Oct. 21, 2021), https://go.usa.gov/xtrhv (stating, "As the direct gateways to this essential and ubiquitous tool, internet service providers ('ISPs') can monitor and record their customers' every online move, giving them the ability to surveil consumers and amass large amounts of information on them as they go about their daily lives."). *See also* Karen Scarfone & Peter Mell, National Institute of Standards

(continued….)

actors, which potentially could include Internet Service Providers (ISPs), can breach information security in multiple ways. Such breaches or attacks can be characterized, at a simplified level, in two categories: (1) active attacks consisting of intrusion into victims' networks or other deliberate disruption of data and control of signaling operations, such as denial of service in the target's network(s);[432] and (2) passive attacks, involving eavesdropping and monitoring of data to collect information.[433] Active attacks tend to exploit weaknesses in standardized protocols and their implementation.[434] In the case of active attacks, ISPs in the role of bad actors can gain unauthorized access to a victim's data via overt network operation (*e.g.*, through BGP hijacking).[435] This can be accomplished from any location on the Internet and used to extract metadata or other information or to manipulate the intercepted data.[436] In the case of passive attacks, an ISP can take advantage of its designated role as a service provider in carrying customer traffic, but exploit the trust of its customers and other ISPs to whom such traffic pertains by monitoring, observing, and collecting customers' data and/or metadata from said traffic. Passive monitoring can compromise both unencrypted and encrypted traffic.[437] In particular, passive monitoring can turn into a

(Continued from previous page)
and Technology (NIST), *Guide to Intrusion Detection and Prevention Systems (IDPS)*, NIST Special Publication 800-94 (2007), https://go.usa.gov/xeFMV (*NIST Guide to Intrusion Detection and Prevention Systems*) (discussing types of intrusions and best practices for intrusion detection and prevention). 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://go.usa.gov/xeFM6.

[432] *See, e.g.*, Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, Wired (Oct. 21, 2016), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ (discussing distributed denial of service attack (DDoS) against Dyn, an Internet infrastructure company, that subsequently caused outages for several parts of the Internet).

[433] *See* Richard Derbyshire et al., *An Analysis of Cyber Security Attack Taxonomies*, 2018 IEEE European Symposium on Security and Privacy Workshops, 153-161 (2018), https://ieeexplore.ieee.org/document/8406575 (discussing the classification of cyberattacks by defining the components of cyberattacks and assessing the effectiveness of cyberattack classifications); Chris Simmons et al., *AVOIDIT: A Cyber Attack Taxonomy* (2009), https://nsarchive.gwu.edu/sites/default/files/documents/4530310/Chris-Simmons-Charles-Ellis-Sajjan-Shiva.pdf (proposing a new taxonomy to aid in identifying and defending against cyberattacks); *see also* Ismail BuTun et al., *Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures,* IEEE Communications Surveys & Tutorials, Vol. 22, No. 1, 616-644 (2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8897627 (categorizing attacks towards Wireless Sensor Networks and Internet of Things as "Passive Attacks" and "Active Attacks" and identifying security solutions).

[434] *See, e.g.*, Gyuhong Lee, et. al., *This is Your President Speaking: Spoofing Alerts in 4G LTE Networks*, MobiSys '19: Proceedings of the 17th Annual International Conference on Mobile Systems, Applications, and Services, 404-416 (2019), https://doi.org/10.1145/3307334.3326082 (addressing one example of an exploitation of a network standard and its implementation).

[435] *See infra* para. 99 (discussing BGP hijacking).

[436] *See, e.g.*, Henry Birge-Lee et al., *Bamboozling Certificate Authorities with BGP*, SEC '18: Proceedings of the 27th USENIX Conference on Security Symposium, 833–849 (2018), https://www.princeton.edu/~pmittal/publications/bgp-tls-usenix18.pdf.

[437] In the case of unencrypted end-to-end traffic, monitoring can lead to simply viewing, copying, or even altering information (data and/or voice) if no integrity protection is present. *See* Internet Engineering Task Force (IETF), *Request for Comments: 6071, Category: Informational, IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap* (February 2011), https://www.rfc-editor.org/info/rfc6071. In the case where end-to-end encryption of data is present, monitoring can extract information from metadata that are derived from encrypted traffic or through brute force decryption. *See* Alireza Bahramali et al., *Practical Traffic Analysis Attacks on Secure Messaging Applications*, Network and Distributed Systems Security (NDSS) Symposium 2020 (May 2020), https://arxiv.org/pdf/2005.00508.pdf (discussing how metadata can be useful to decrypt encrypted data); *see also* Albert Kwon et al., *XRD: Scalable Messaging System with Cryptographic Privacy*, Proceedings of the 17th USENIX Symposium on Networked Systems Design and Implementation, 759-776 (2020),

(continued….)

more serious form of covert surveillance called "pervasive monitoring," which network service providers are well-situated to perform.[438] For example, as part of network management—particularly security management—an ISP such as CUA can use tools to identify network intrusion[439] or perform deep packet inspection in the absence of encryption.[440] These tools can be leveraged to further enable CUA to have access to content, such as listening to conversations, and possibly use this information to engage in espionage, use the information contrary to U.S. interests, or for any other unauthorized activities.

94. As discussed below, CUA's ability as an ISP to conduct active attacks and passive monitoring raises significant law enforcement and national security risks associated with and facilitated by its current services offered pursuant to section 214 authority, IPLC and IEPL. Customers of IPLC and IEPL services are susceptible to both active attacks and passive monitoring by CUA. With respect to active attacks, as described above, CUA is uniquely positioned as an ISP to access confidential customer information. With respect to passive monitoring, CUA can monitor, observe, and collect traffic sent to and/or from its customers in a manner that leaves no trace of having done so and without its customers' authorization or knowledge. CUA has the ability to conduct passive monitoring through its IPLC and IEPL services, which could provide CUA with access to raw data, including their content, in cases where its customers have not incorporated an additional level of end-to-end encryption.[441] With respect to its MPLS VPN service, CUA has the ability, by using the equipment of its customers and/or misrouting, to perform passive attacks by collecting traffic that traverses its network, derive metadata from this traffic,[442] and attempt to decrypt client-encrypted traffic to access the content at a time and location of CUA's choosing. It could also do this via diverting U.S. traffic through extraneous paths via misrouting, using this active technique to realize a passive attack on the traffic to which it thus gains access. As noted above, CUA's ability to combine its section 214 services and those that do not require section 214 authority, makes CUA more attractive as a service provider to U.S. customers than if it did not offer such

(Continued from previous page)
https://www.usenix.org/system/files/nsdi20-paper-kwon.pdf (presenting a metadata private messaging system that provides cryptographic privacy); Katie Terrell Hanna, Definition: *brute-force attack*, TechTarget, https://searchsecurity.techtarget.com/definition/brute-force-cracking.

[438] The Internet Engineering Task Force (IETF) describes pervasive monitoring as covert "surveillance through intrusive gathering of protocol artefacts, including application content, or protocol metadata such as headers," which can include "[a]ctive or passive wiretaps and traffic analysis, (e.g., correlation, timing or measuring packet sizes), or subverting the cryptographic keys used to secure protocols . . . ." Internet Engineering Task Force (IETF), *Request for Comments: 7258, Category: Best Current Practice, Pervasive Monitoring Is an Attack* at 2 (May 2014), https://www.rfc-editor.org/info/rfc7258; *id.* (identifying pervasive monitoring as "an attack on the privacy of Internet users and organisations"). In addition, the Internet Architecture Board (IAB) recognizes that an entity that is well-situated, such as a network service provider, may be an "observer" in that it "is able to observe and collect information from communications, potentially posing privacy threats, depending on the context." *See* Internet Architecture Board (IAB), *Request for Comments: 6973, Category: Informational, Privacy Considerations for Internet Protocols* at 7, 11-12 (July 2013), https://www.rfc-editor.org/info/rfc6973. The IAB notes that an attacker such as an "eavesdropper" can "passively observe[] an initiator's [sender's] communications without the initiator's knowledge or authorization" in the context of compromising privacy. *Id*. at 7, 11-12.

[439] *See*, *e.g.*, *NIST Guide to Intrusion Detection and Prevention Systems*, *supra* note 431, Section 2.

[440] *See* Ericka Chickowski, *Deep packet inspection explained*, AT&T (Oct. 2, 2020), https://cybersecurity.att.com/blogs/security-essentials/what-is-deep-packet-inspection.

[441] While we recognize that CUA may offer encryption of the traffic that enters its infrastructure or customer premise equipment under its management, the ingress data are unencrypted and therefore can be copied, stored, and/or manipulated.

[442] *See* Joseph Cox, *How Data Brokers Sell Access to the Backbone of the Internet*, Vice (Aug. 24, 2021), https://www.vice.com/en/article/jg84yy/data-brokers-netflow-data-team-cymru (noting how ISPs can trace traffic through virtual private networks).

a suite of services, which in turn may drive more customers and more traffic to CUA's networks and thus present more opportunities to perform active or passive attacks.

95. *Security Threats Related to CUA's Provision of IPLC, IEPL, and Services Based on Internet Routing.* IPLC and IEPL are lower layer network services that support point-to-point communications and operate independently of the IP network layer, providing transport to IP traffic. The services are used to extend the underlying physical network (*e.g.*, Ethernet) to enable connectivity between computers in distant locations (*e.g.*, connecting servers and routers without the use of IP routing).[443] Depending on the service management responsibilities of CUA, the IPLC and IEPL services may or may not include end-to-end encryption. Even if encryption is available, it nevertheless does not provide the customer with protection from unauthorized access by the ISP if the ISP is the party that performs the encryption. That is, if CUA performs the encryption, it still has access to the unencrypted data because it manages the keys needed to encrypt and decrypt this data.[444]

96. While IPLC and IEPL operate below the IP layer, other services that rely on Internet routing to forward traffic from source to destination still present additional risks. Forwarding of IP traffic and BGP routing do not require section 214 authority and could continue to be offered by CUA or any of its parent entities irrespective of section 214 authority. However, while interdomain routing, as supported by BGP, is not a service subject to section 214 authority, it is critical in supporting various services that may require such authority. Such services may include MPLS VPN, DIA, IDC, cloud services, and IP transit services with regard to IP traffic sent to CUA's network, and potentially may include IPLC and IEPL services depending on how they are deployed internally by CUA. Additionally, CUA, like any ISP, can monitor its customers' traffic. As noted above, CUA's provision of an enhanced suite of services, some pursuant to its section 214 authority, heightens the national security and law enforcement risks presented by its ensuing ability to attract more customers whose traffic would then be subject to the vulnerability described here. We find that revocation of CUA's section 214 authority therefore could substantially diminish CUA's ability to engage in conduct harmful to the national security and law enforcement interests of the United States.

97. CUA has offered no persuasive argument to dispel the significant concerns raised in the *Institution Order* that CUA "could maliciously or accidentally redirect to China VoIP data traffic from an MNO or MVNO by mounting a BGP route attack originated at or through one of its 11 U.S. PoPs, for example, from [CUA's] BGP routers, a scenario enabled by [CUA] using BGP as is customary with its peering partners."[445] This threat is more than theoretical.[446] Indeed, the *Institution Order* observed that "in an independent analysis of attacks initiated by foreign networks that targeted U.S. mobile users and devices . . . , a component of China Unicom was identified as the likely source of more such attacks than any other provider in the world from May 2018 to December 2019."[447] In fact, the Executive Branch

[443] *Institution Order*, 36 FCC Rcd at 6351, para. 46.

[444] In the *China Telecom Americas Order on Revocation and Termination*, the Commission stated that "(w)hile we recognize that CTA may offer encryption of the traffic that enters its infrastructure or customer premise equipment under its management, the ingress data are unencrypted and therefore, through the use of malware or purposeful bad cyber hygiene, can be copied, stored, and/or manipulated." *China Telecom Americas Order on Revocation and Termination* at *30, n.373.

[445] *Institution Order*, 36 FCC Rcd at 6348, para. 42.

[446] *See* Kotikalapudi Sriram, Doug Montgomery, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST Special Publication 800-189 (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-189.pdf (Resilient Interdomain Traffic Exchange) (discussing BGP vulnerabilities, stating that "A BGP prefix hijack occurs when an autonomous system (AS) accidentally or maliciously originates a prefix that is not authorized (by the prefix owner) to originate.").

[447] *Institution Order*, 36 FCC Rcd at 6348, para. 42 (citing Exigent Media, *Far From Home: Active Foreign Surveillance of U.S. Mobile Users 2018-2019: Threat Intelligence Report*, 13, 16, https://img1.wsimg.com/blobby/go/bd1a4ad4-9ec5-4725-8720-

(continued….)

agencies state that CUA "advertises BGP routing information to peering partners, including major Tier 1 [ISPs]" and that "CUA's U.S. operations, particularly its 11 PoPs in the United States, provide [Chinese] government-sponsored actors with openings to disrupt or misroute U.S. data and communications traffic, enabling its collection."[448] For instance, misrouting may occur due to routers deliberately configured to implement a routing architecture that facilitates unauthorized data access. CUA, like any ISP, uses standard routing protocols such as BGP,[449] to route traffic across the Internet. Based on analysis of publicly available BGP data,[450] we observe that CUA's network appears to currently have five interconnection partners, including "CHINA UNICOM Industrial Internet Backbone" and "China Organizational Name Administration Center" (CONAC).[451] CUA and CU can use their BGP routing policies[452] to redirect traffic originally destined to CUA's IP address prefixes in the United States[453] to instead traverse CU's network outside the United States.

98. Importantly, CUA and CU's BGP routing can be used to redirect the traffic through China rather than having that traffic remain in the United States, and this provides another opportunity for this traffic to be readily captured, examined, and/or altered.[454] The risks associated with misrouting of and any unauthorized access to such traffic are particularly significant because such activities may not be readily detected by CUA's customers or by end users that may send traffic to CUA's customers. To ascertain CUA's misrouting of Internet traffic, CUA's customers would need to avail of a variety of

(Continued from previous page)
3578900df157/downloads/Far%20From%20Home%20Threat%20Intelligence%202018-2019.pdf?ver=1625674073997 (last visited Jan. 26, 2022)).

[448] Executive Branch Letter at 35.

[449] *Resilient Interdomain Traffic Exchange*, *supra* note 446 ("BGP is the control protocol used to distribute and compute paths between the tens of thousands of autonomous networks that comprise the Internet.").

[450] *See* CAIDA AS Rank, *China Unicom (Americas) Operations, Ltd*, https://asrank.caida.org/asns/19174 (listing five interconnection partners) (last visited Jan. 26, 2022). CAIDA collects data on interconnections and infers relationships between service providers. *See* CAIDA, *AS Relationships*, https://www.caida.org/catalog/datasets/as-relationships/. As such, CAIDA does not have access to information pertaining to the exact nature of CUA's relationships with its interconnection partners, but rather *infers* CUA's relationships to these entities to be interconnection relationships.

[451] *See* CAIDA AS Rank, *China Unicom (Americas) Operations, Ltd*, *supra* note 450 (identifying and inferring "Level 3 Parent, LLC," "Cogent Communications," "MCI Communications Services, Inc. d/b/a Verizon Business," "CHINA UNICOM Industrial Internet Backbone" as transit providers, and "CONAC (China Organizational Name Administration Center)" as a transit customer of "China Unicom (Americas) Operations Ltd"). We also note that Hurricane Electric views these networks as peers. *See* Hurricane Electric Internet Services, AS19174 China Unicom (Americas) Operations Ltd, https://bgp he net/AS19174#_peers (last visited Jan. 26, 2022).

[452] *See* ThousandEyes, *Peering Policy—Peering Policy Overview and Technical Requirements*, https://www.thousandeyes.com/learning/techtorials/peering-policy (last visited Jan. 26, 2022) (explaining peering policies and their use by network operators, including BGP routing).

[453] CUA has been assigned several IP address prefixes by the American Registry for Internet Numbers (ARIN). *See* American Registry for Internet Numbers (ARIN), *ARIN Whois/RDAP*, https://search.arin net/rdap/ (search for 199.102.92.0, 199.102.95.0, 207.254.176.0, 207.254.176.0, 207.254.177.0, 207.254.179.0, 207.254.180.0, 207.254.186.0, 207.254.189.0, 207.254.190.0) (last visited Jan. 26, 2022). An IP address prefix is a range of addresses assigned to a network or provider. A similar analogy would be the 1200 block of Main Street, where 12 is the prefix that encompasses 1200 to 1299. *See* Network Working Group, *Request for Comments: 1930, Category: Best Current Practice, Guidelines for creation, selection, and registration of an Autonomous System (AS)*, Sec. 3. Definitions (March 1996), https://datatracker.ietf.org/doc/html/rfc1930#section-3.

[454] If traffic to or from CUA's network is routed via CUG's network, the traffic can travel anywhere on CUG's network while in transit.

tracking counter measures, perhaps including periodic traceroutes.[455] This threat of misrouting could be realized if CU, while transmitting the traffic sent to it by CUA, could engage in unauthorized access or copying either by using CU's facilities within the United States[456] or by routing this traffic through China. For example, if Internet traffic is destined to follow the shortest path between Philadelphia and Los Angeles, the traffic normally would be expected to be routed wholly within the United States, as opposed to being routed from Philadelphia, through Beijing, and then to Los Angeles. Examples such as this, in which traffic that originates from and is destined to networks in the United States but is routed outside of the United States during transit, may be a form of misrouting that raises significant national security and law enforcement concerns.

99. We recognize that various ISPs' decisions regarding BGP routing policies result in different routes across the Internet, and the choice of specific routes may result in traffic transiting through networks that do not have the same protections of data that exist in the United States. For example, CUA's BGP routing policies may result in data transiting CU's network before it reaches CUA. To extend the example further, it is also possible for an Autonomous System (AS) to announce false routing information that deliberately diverts traffic away from expected BGP routes.[457] This is known as "BGP hijacking" or "route leaks."[458] These anomalous routes, unless detected in a timely fashion, may then cause Internet traffic to transit network paths that the customer and its provider did not intend the traffic to traverse, or alternately, "blackhole"[459] traffic to the customer. Both BGP hijacking or route leaks incidents may occur on either an intentional (*i.e.*, malicious) or accidental basis, and it may be impossible to distinguish between the two cases.[460] This in turn makes it easier to claim that a BGP

[455] Traceroute is a network diagnostic tool used to track the path taken by an IP packet from source to destination. *See* ThousandEyes, *What is Traceroute & What is it For?*, https://www.thousandeyes.com/learning/glossary/traceroute (last visited Jan. 26, 2022). Network traffic monitoring, including BGP and route monitoring, is a security and reliability service offered by network providers and third parties. *See Monitor BGP Routes To and From Your Network*, ThousandEyes, https://www.thousandeyes.com/solutions/bgp-and-route-monitoring (last visited Jan. 26, 2022).

[456] *See supra* note 453 (specifying the IP addresses assigned to CUA in the United States).

[457] *See Resilient Interdomain Traffic Exchange*, *supra* note 446.

[458] *See* K. Sriram et al., *Request for Comments: 7908, Category: Informational, Problem Definition and Classification of BGP Route Leaks*, Internet Engineering Task Force (IETF) (June 2016), https://www rfc-editor.org/rfc/rfc7908 html (*Problem Definition and Classification of BGP Route Leak*). We note that the term "prefix hijacking" is more exact but does not include all BGP-based attacks. *See* Kevin Butler et al., *A Survey of BGP Security Issues and Solutions*, Proceedings of the IEEE, Vol. 98, No. 1 at 100-122 (2010), https://www.cise.ufl.edu/~butler/pubs/bgpsurvey.pdf. In general, leaks can be regarded as deliberate or accidental misconfigurations of BGP routers and policies that allow routes (and corresponding traffic) to travel over unintended paths. *See Problem Definition and Classification of BGP Route Leak*.

[459] A route blackhole occurs when traffic never reaches its destination. *See, e.g.*, RIPE NCC, *YouTube and Pakistan Telecom*, https://youtu.be/IzLPKuAOe50 (Feb. 28, 2008) (discussing a YouTube outage and how it was seen by RIPE NCC's Routing Information Service); Hari Balakrishnan, *How YouTube was "Hijacked,"* Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science at 1 (May 2009), http://web mit.edu/6.02/www/s2012/handouts/youtube-pt.pdf.

[460] New tools make detection of false origination increasingly feasible, but their deployment is limited. NIST has described recent developments, including a tool called the NIST Resource Public Key Infrastructure (RPKI) Monitor. *See* Lilia Hannachi et al., *NIST RPKI Deployment Monitor*, NIST (updated Apr. 27, 2021), https://go.usa.gov/xeFMh. *See also* The United Kingdom Network Operators' Forum (UKNOF), *UKNOF45 – Artemis: an Open-source Tool for Detecting BFP Prefix Hijacking in Real Time*, (Jan. 19, 2020, https://www.youtube.com/watch?v=j-W_960F_xE (addressing deployment of these tools). In short, BGP routing remains susceptible to hacking, notwithstanding continuous improvements in methods to verify routing. This vulnerability further reinforces the importance of an ISP's trustworthiness. *See* Yu Zhang et al., *A Framework to*

(continued….)

hijack or route leak is accidental, even if it is not. Further, a bad actor can obtain information through routing leaks from both unencrypted and encrypted traffic.[461] For example, researchers have demonstrated how, through BGP hijacks, bad actors can reveal the identity, in the form of source and destination IP addresses, of a significant percentage of customers on a network specifically designed to enable anonymous communication over the Internet (e.g., enable website visits without tracking by third parties).[462] In its role as a provider of IPLC, IEPL and other Internet-based services, CUA has a clear opportunity to engage in active or passive monitoring, or to misroute communications as described above. This opportunity, when combined with CUA's ultimate ownership and control by the Chinese government, poses an unacceptable risk to U.S. national security and law enforcement interests.

100. *Security Threats Related to CUA's Physical Presence in the United States.* The potential for a service provider to engage in active and passive monitoring, misrouting of communications, and other threats to U.S. national security and law enforcement interests is influenced by the physical proximity of CUA's provider network to other U.S. providers. We note that every network service provider "sits at a privileged place in the network . . . from which it enjoys the ability to see at least part of every single packet sent to and received from the rest of the Internet."[463] Individuals, companies, and anyone else using CUA's network services entrust their data and communications to CUA, the network service provider. It is critical that a network service provider understand the significance of this trusted role. As stated simply and even predating telecommunications services, anyone entrusted with possession of property owned by another has "an opportunity of undoing all persons who have had dealings with them," by engaging in malicious activity "and yet doing so in a clandestine manner, as would not be possible to be discovered."[464] Trusted relationships with service providers remain critical today;[465] in its

(Continued from previous page)
Quantify the Pitfalls of Using Traceroute in AS-Level Topology Measurement, IEEE Journal on Selected Areas in Communications, Vol. 29, Issue 9 at 1822-1836 (Oct. 2011), https://ieeexplore.ieee.org/document/6027864 (identifying errors in traceroute measurement in AS-level topology inference).

[461] *See China Telecom Americas Order on Revocation and Termination* at *32, para. 86 & n.392.

[462] *See* Yixin Sun et al., *Securing Internet Applications from Routing Attacks*, Communications of the ACM, Vol. 64 No. 6 at 86-96 (June 2021), https://cacm.acm.org/magazines/2021/6/252822-securing-internet-applications-from-routing-attacks/fulltext; Tor Project, Inc., https://www.torproject.org ("Tor Browser isolates each website you visit so third-party trackers an ads can't follow you. . . . Tor Browser prevents someone watching your connection from knowing what websites you visit.") (last visited Jan. 26, 2022).

[463] Letter from Paul Ohm, Professor, Georgetown University Law Center, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 16-106 Attach. at 3 (filed June 19, 2016) (Statement of Paul Ohm, Professor, Georgetown University Law Center and Faculty Director, Georgetown Center on Privacy and Technology Before the Subcommittee on Communications and Technology, Committee on Energy and Commerce, U.S. House of Representatives (June 14, 2016)) (Paul Ohm Statement); *see NIST Guide to Intrusion Detection and Prevention Systems*, *supra* note 431 (discussing Deep Packet Inspection).

[464] *Coggs v. Bernard*, (1703) 2 Ld Raym 909, 918, 92 ER 107 (articulating the historic concern of vulnerability of customers who entrust goods to common carriers); *China Telecom Americas Order on Revocation and Termination* at *34, n.403. Communications law has historically recognized the unique trust relationship between customers and network service providers, and their vulnerability to bad acts by providers. *See National Ass'n of Regulatory Utility Commissioners v. FCC (NARUC I)*, 525 F.2d 630, 640, 641 (DC Cir. 1976) (describing a historical rationale for the treatment of common carriage as "the lack of control exercised by shippers or travellers over the safety of their carriage," and describing the relationship of the carrier to its customers as one of "public trust"). *See also* Barbara Cherry, The Crisis in Telecommunications Carrier Liability: Historical Regulatory Flaws and Recommended Reform 12 (1999) ("*Coggs v. Bernard* is considered the case on which the modern law of bailees is based."); Oliver Wendell Holmes, The Common Law, Lecture V: The Bailee at Common Law 164 (1881); Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), https://go.usa.gov/xtYGu (discussing users' lack of trust in the security of their data and communications on the Internet).

privileged role as a network service provider, with its unconstrained physical presence in the United States, and with its section 214 authority and non-section 214 service offerings, CUA has significant opportunity to engage in both active attacks and passive or pervasive monitoring.

101. We remain concerned about CUA's physical presence in the United States. CUA has provided no arguments or evidence that dispel these concerns. By directly interconnecting with U.S. networks within the United States, there is a high probability that traffic between U.S. providers will transit CUA's network. For example, if a BGP route announcement for a destination in the United States occurs far away geographically (and topologically from the perspective of BGP), networks *within* the United States may ignore the announcement. This occurs because by the time the announcement reaches a U.S. network, the "hop count"—a standard BGP metric that represents the number of distinct networks to be traversed to a destination—will be excessively large compared to other routes and thus the announcement would not be accepted. In contrast, if an anomalous BGP route announcement occurs at a PoP located in the United States, it is more likely to be accepted and used to route traffic given that the path will have a hop count that is low. This event can cause harm to networks that are topologically closely interconnected to the announcer. Because CUA has a physical presence in the United States, it can make a BGP announcement to connect between two points within the country—for example, between Philadelphia and New York—and the probability that such announcement would be accepted is much greater than if CUA only had assets outside of the United States. In such circumstances, given that there is a greater number of U.S. networks that are potentially available for peering within the United States, rather than outside it, this physical proximity in the United States provides CUA with greater opportunity for access to U.S. communications and thus poses a greater national security and law enforcement risk.

102. A key measure of an international network service provider's physical span or reach is the number and distribution of its PoPs, which are physical locations where the network service provider offers or avails of interconnection or other Internet-related services. CUA's PoPs in the United States are highly relevant to its ability to access, monitor, store, disrupt, and/or misroute communications to the detriment of U.S. national security and law enforcement. The Executive Branch agencies report that "CUA now peers with 26 IP partners for the exchange of Internet traffic and also provides data center, and cloud computing services."[466] The PSI Report notes that CUA has 11 PoPs in the United States, which are colocation facilities leased from third parties where CUA owns and operates routers.[467] A recent review of CUG's website showed 10 PoPs across the United States.[468] CUA's PoPs in the United States are not separate operations unrelated to CUA's telecommunications services, including those that may be provided pursuant to section 214 authority. Rather, CUA's PoPs in the United States provide it with the capability to access and/or manipulate data, while CUA's telecommunications services, including those that may be provided pursuant to section 214 authority, make CUA more attractive as a service provider and thus more likely to obtain traffic that would pass through these PoPs. As we noted in the

(Continued from previous page)

[465] *See* Paul Ohm Statement at 3; Harold Feld, et. al., *Protecting Privacy, Promoting Competition: A Framework for Updating the Federal Communications Commission Privacy Rules for the Digital World*, Public Knowledge (2016), https://publicknowledge.org/policy/protecting-privacy-promoting-competition-white-paper/ (discussing the data that can be gathered by a network service provider from its customers and end users).

[466] Executive Branch Letter at 14.

[467] PSI Report at 81 & n.498 (citing Briefing with China Unicom Americas (Apr. 16, 2020)).

[468] *See* China Unicom Global PoPs, *supra* note 363 (displaying 10 locations in the United States associated with "PoPs"). The website identifies each PoP as "China Unicom Global PoPs." *Id.* (presenting a separate link and corresponding webpage for each PoP, including street address). We note that the locations of the PoPs identified on CUG's website correspond with the locations of the CUA's PoPs as identified in the PSI Report. *See id.* (identifying PoPs in "Ashburn, United States"; "Chicago, United States"; "Dallas, United States"; "Hillsboro, United States"; "Los Angeles, United States"; "Miami, United States"; "New York, United States"; "Palo Alto, United States"; "San Jose, United States"; and "Seattle, United States); PSI Report at 81 & n.498.

Institution Order,[469] the Executive Branch agencies' concerns about CUA's U.S. operations include the fact that, "due to least-cost routing, the communications of U.S. government agencies to any international destinations may conceivably pass through [CUA's] network during transit, even if the agencies are not actual [CUA] customers."[470]

103. An important concern related to a service provider's PoPs is the security of the equipment used by that provider. This concern about network equipment and security has extended across the U.S. Government. For example, the Secure and Trusted Communications Networks Act of 2019 was enacted in 2020,[471] and an Executive Order on Securing the Information and Communications Technology and Services Supply Chain was issued on May 15, 2019.[472] In implementing the Secure and Trusted Communications Networks Act and its amendments, and consistent with its duties as established by Congress "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 communication,"[473] the Commission has required that service providers receiving Universal Service Fund (USF) support remove from their networks any equipment by "covered providers" that have been deemed a security risk to the U.S. communications network.[474] This requirement applies to all telecommunications service providers receiving USF support and is not tailored to apply only to providers that may be deemed a security threat. Based on the record, CUA's list of equipment providers includes {[ ]} and, among other equipment, these providers are sources of {[ ]} for CUA.[475]

104. Finally, in the course of providing section 214 services and those that do not require such authority, CUA, like any similarly situated provider, can have both physical and remote access to its customers' equipment needed to provide such services. This physical access would present opportunities for CUA to monitor and record sensitive information, thus creating a significant risk of harm. CUA could cause this harm while managing its customers' equipment in support of the services it provides, including those pursuant to section 214 authority. This is exactly the type of opportunity that bad actors seek.

---

[469] *Institution Order*, 36 FCC Rcd at 6347, para. 41.

[470] Executive Branch Letter at 31.

[471] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601–1609) (Secure and Trusted Communications Networks Act).

[472] Executive Order No. 13873 of May 15, 2019, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22689 (May 17, 2020) (Executive Order 13873); Notice of May 11, 2021, Continuation of the National Emergency With Respect to Securing the Information and Communications Technology and Services Supply Chain, 86 Fed. Reg. 26339 (May 13, 2021) (continuing for one year the national emergency declared in Executive Order 13873 with respect to securing the information and communications technology and services supply chain).

[473] 47 U.S.C. § 151.

[474] *Protecting Against National Security Threats Order,* 34 FCC Rcd at 11433, para. 26. *See generally 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 (PSHSB 2020) (*PSHSB Huawei Designation Order*); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs – ZTE Designation*, PS Docket No 19-352, Order, 35 FCC Rcd 6633 (PSHSB 2020) (*PSHSB ZTE Designation Order*). *See also* Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, 134 Stat. 1182, 1652 (2020) (amending the Secure and Trusted Communications Networks Act to limit the use of reimbursement funds for equipment identified in the *Protecting Against National Security Threats Order*, *PSHSB Huawei Designation Order*, and *PSHSB ZTE Designation Order*, to Huawei and ZTE).

[475] CUA Response to *Order to Show Cause*, Business Confidential Exh. 5.

DHS' Cybersecurity and Infrastructure Security Agency has received multiple reports of bad actors actively exploiting trust relationships in information technology service provider networks.[476]

105. *Additional Misrouting Concerns Involving Section 214 and Non-Section 214 Services.* CUA's provision of IPLC, IEPL, and its offering of non-section 214 MPLS VPN services, whether provided individually or as part of a package, present opportunities to (1) access customer metadata, (2) access customer data including all content, and (3) misroute communications (at layers below IP). Notably, these harms could occur without the customer's authorization or knowledge.

106. With respect to CUA's IPLC and IEPL service, the potential for misrouting exists with two mechanisms by which CUA may send traffic: (1) directly between endpoints using a point-to-point Ethernet circuit or (2) over its IP network.[477] The first mechanism, with a point-to-point Ethernet circuit, would require using long-haul transport infrastructure (*e.g.*, fiber) from one of CUA's Internet backbone providers, such as its indirect parent, CU.[478] In this case, if CUA uses CU's network, the risks associated with misrouting are those attributable to CU in its role as an Internet backbone provider. The second mechanism, using IP to send the traffic over the Internet, would involve BGP routing, as described above, and require using one of CUA's transit providers, such as its indirect parent, CU.[479] In this case, the risks associated with misrouting are related to how the provider of the IX service connects with other similar providers to send traffic. As a provider of IEPL service as well as other services under its section 214 authority, CUA would choose which of these two mechanisms to employ. In the event CUA chooses or is required to pursue either mechanism with involvement by CU, significant risks would follow, as CU could easily and without knowledge of CUA's customers route U.S. traffic through non-U.S. facilities, including those in China. In addition to the risk of misrouting, services such as IPLC and IEPL are vulnerable to passive monitoring due to physical limitations that require intermediate repeaters to retransmit data towards the final endpoint of the service. These repeaters allow a provider to extend a service across thousands of miles, but they also introduce the vulnerability for a service provider to illegally (or in violation of customer contracts) eavesdrop on traffic through monitoring ports to capture it or forward it to another destination for eventual capture.[480]

107. With respect to CUA's MPLS VPN service, which CUA contends it does not offer pursuant to section 214, this also provides CUA with the ability and opportunity to misroute traffic and/or forward traffic to CU, its indirect parent, that can then act on its ability and opportunity to misroute and/or

---

[476] *See* U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, *APTs Targeting IT Service Provider Customers*, https://us-cert.cisa.gov/APTs-Targeting-IT-Service-Provider-Customers ("The Cybersecurity and Infrastructure Security Agency (CISA) has received multiple reports of advanced persistent threat (APT) actors actively exploiting trust relationships in information technology (IT) service provider networks around the world.") (last visited Jan. 26, 2022).

[477] Forwarding IEPL traffic over IP networks can be accomplished in several ways. One example is Ethernet over IP (EoIP). *See Keenetics, Setting up IPIP, GRE and EoIP Tunnels* (June 28, 2021), https://help.keenetic.com/hc/en-us/articles/115002715029-Setting-up-IPIP-GRE-and-EoIP-tunnels.

[478] *See supra* para. 97 (addressing CUA's Internet backbone providers, which include CU).

[479] *See* China Unicom Global, Network & Services, https://network.chinaunicomglobal.com/#/district/north-america (last visited January 26, 2022). For an example of a PoP listed on CUA's website that links to CUG, *see* China Unicom Global (MAP), https://network.chinaunicomglobal.com/#/city/dallas-united-states (last visited Jan. 26, 2022).

[480] *See, e.g.,* Marija Furdek et al., Vulnerabilities and Security Issues in Optical Networks, 2014 16th International Conference on Transparent Optical Networks (July 2014), https://www.researchgate.net/publication/269268194_Vulnerabilities_and_security_issues_in_optical_networks (providing a comprehensive overview of security issues in state-of-the-art optical networks, identifying and describing the main vulnerabilities of current and future networks, and outlining potential methods of attack that could exploit these vulnerabilities).

forward traffic in ways that enable espionage or are otherwise contrary to U.S. national security and law enforcement interests.[481] Due to CUA's transit relationship with CU, and its susceptibility to exploitation, influence, and control by the Chinese government, the ability and opportunity to misroute and/or forward traffic raise substantial and significant national security and law enforcement concerns. As discussed above, CUA advertises its access to its indirect parent CU's Internet backbone, highlighting its access to the segment of the Internet within China and interconnections with other Chinese carriers.[482]

108. We reject CUA's argument that revocation of its section 214 authority would not necessarily address the national security and law enforcement concerns raised by the Commission. CUA maintains that "(w)hile revocation would remove CUA as a provider of services, it would not remove the demand for such services" and that "U.S. businesses require communications between the U.S. and China, the world's two largest economies. . . . the customers will pivot to other providers."[483] CUA contends that "if the Commission is successful in revoking the authorizations of all carriers with Chinese government interests, there would not be any carriers with direct access between the U.S. and Chinese markets," and that "the Commission's actions will force U.S. customers to purchase indirect access from other carriers that will simply connect with an affiliate of a Chinese domestic carrier in another country."[484] CUA argues that "[t]his is clearly contrary to the public interest as the cost to U.S. customers will increase and network performance would be adversely impacted due to the additional routing of the traffic through another country."[485]

109. We recognize the demand for communications between the United States and China, both for business and individual customers. We further recognize that communications that originate from or terminate in China—as part of a telecommunications service, IP transit, or other communications—will necessarily involve connection with a service provider that is majority-owned by the Chinese government, with all of the aforementioned risks that such connection entails. At the same time, we take seriously the Commission's mandate to protect the national security and law enforcement interests of the United States in its communications and related infrastructure. Accordingly, we take actions, including the revocation of section 214 authority, to limit these threats from telecommunications providers with operations in the United States, cognizant of the potential costs. We believe that these costs—*e.g.*, due to less-efficient routing of traffic—are significantly outweighed by the benefits from this action which protects U.S. national security and law enforcement interests.

110. We find that CUA's provision of the services described above—including those that require and those that do not require section 214 authority—raises significant national security and law enforcement risks to the United States. These services, offered individually or as part of a suite of services, when combined with CUA's physical presence in the United States, CUA's relationship with its parent entities,[486] and CUA's vulnerability to the exploitation, influence, and control of the Chinese government,[487] present an unacceptable risk to the U.S. communications network requiring revocation of its section 214 authority. Finally, as noted above, CUA argues that "[i]n the event that CUA's section 214 authorizations are revoked, it believes that other than the MVNO services, it can continue to provide

[481] As described above, CUA peers directly with CU. *See supra* note 451 (noting that CUA peers with "CHINA UNICOM Industrial Backbone"); *see* ASRank, https://asrank.caida.org/asns?asn=19174&type=search.

[482] *See supra* notes 428, 430.

[483] CUA Response to *Institution Order* at 27.

[484] *Id*. at 27-28.

[485] *Id*. at 28.

[486] *See supra* note 363 (addressing CUA's U.S. Points of Presence, colocation facilities, and cloud exchanges).

[487] *See supra* Section III.B.1.

all of its remaining services on a private carriage basis, without a section 214 authorization."[488] We decline to address the merits of this argument given the lack of record evidence on this issue.[489] Pursuant to this order, we revoke CUA's section 214 authority and accordingly, CUA must discontinue all common carrier services offered pursuant to section 214 authority.[490] We note, however, that entities solely providing private line service may nevertheless be considered common carriers if they offer their services directly to the public or to such classes of users as to be effectively available directly to the public.[491]

3. CUA's Past Representations to the Commission and Congress Support Revocation of its Section 214 Authority

111. We find that CUA's past representations to the Commission and Congress require us to find—independent of our separate concerns about the intent and ability of the Chinese government to use its control of CUA in ways that pose serious risks to critical U.S. national security and law enforcement interests—that the public interest, convenience, and necessity is not served by CUA's retention of its section 214 authority. First, we find that CUA failed to provide the Commission with crucial information that was disclosed to the Senate Subcommittee and published in its PSI Report. Specifically, CUA failed to provide information relevant to CUG's role {[ ]}[492] in CUA's management and operations, and failed to disclose a confidentiality agreement.[493] Second, CUA did not fully respond to several questions in the *Order to Show Cause* and the *Institution Order* relevant to its ownership and the provision of section 214 telecommunications services.[494] Third, CUA failed to comply with the terms of its ISPC assignments and the Commission's rules concerning the filing of notifications for certain transactions. Specifically, with respect to the Commission's rules, CUA's failure to comply with the Commission's rules resulted in the International Bureau's reclamation of CUA's three ISPCs[495] and our finding that CUA was not in

---

[488] CUA Response to *Institution Order* at 45. CUA adds that "[o]ther than its MVNO services, CUA provides all of its other telecommunication services pursuant to individually tailored and negotiated contracts." CUA Response to *Institution Order* at 45, n.147.

[489] *See supra* note 361. As stated above, CUA fails to provide the detailed and verifiable factual support needed for the Commission to evaluate its claim.

[490] CUA is required to discontinue domestic "Dedicated Private Line circuits" and domestic EPL and any other service CUA is currently providing under section 214 authority.

[491] *See National Ass'n of Regulatory Utility Com'rs v. FCC*, 533 F.2d 601, 608-609 (D.C. Cir. 1976) (describing the situations in which a carrier may be considered a common carrier) (*NARUC II*). Specifically, the court in *NARUC II* stated that "[a]n examination of the common law reveals that the primary sine qua non of common carrier status is a quasi-public character, which arises out of the undertaking 'to carry for all people indifferently. . . .' This does not mean that the particular services offered must practically be available to the entire public; a specialized carrier whose service is of possible use to only a fraction of the population may nonetheless be a common carrier if he holds himself out to serve indifferently all potential users. Nor is it essential that there be a statutory or other legal commandment to serve indiscriminately; it is the practice of such indifferent service that confers common carrier status. That is to say, a carrier will not be a common carrier where its practice is to make individualized decisions in particular cases whether and on what terms to serve. A second prerequisite to common carrier status . . . is the requirement formulated by the FCC and with peculiar applicability to the communications field, that the system be such that customers 'transmit intelligence of their own design and choosing.'" *Id*.

[492] CUA Response to *Institution Order*, Business Confidential Exh. 3.

[493] *See* PSI Report at 49; *Institution Order*, 36 FCC Rcd at 3363-65 at paras. 50-51.

[494] *Institution Order*, 36 FCC Rcd at 6353, para. 49.

[495] Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC, International Bureau, to Robert E. Stup, Jr. and Paul C. Besozzi, Counsel for China Unicom (Americas) Operations Limited, DA 21-227 (Mar. 10, 2021) (on file in GN Docket No. 20-110, File Nos. SPC-NEW-20030730-00031, SPC-NEW-20031009-

(continued….)

compliance with our *pro forma* rules for approximately ten years.[496] CUA's transparency and truthfulness with the Commission and other U.S. government agencies, as well as its ability to comply with the Commission's rules, are essential characteristics to demonstrate that CUA's retention of its section 214 authority continues to serve the public interest, convenience, and necessity.[497] This trust is paramount given that, as noted above, carriers sit at a privileged position to provide critical telecommunications services in the United States.[498] Although CUA had several opportunities, CUA provided no evidence in the record to dispel the concerns that were identified in the *Institution Order*. We find that CUA's representations to the Commission and Congress demonstrate CUA's lack of "transparency, reliability, and ability to comply with Commission rules."[499] CUA's representations also show CUA's failure "to cooperate with the Executive Branch agencies and the U.S. government generally."[500] Based on the record evidence, we find that CUA cannot be trusted to cooperate with the Commission or the Executive Branch agencies, to comply with the Commission's rules, and, importantly, to assist with the Commission's statutory obligations to act "for the purpose of the national defense [and] for the purpose of promoting safety of life and property."[501]

a. Omission of Crucial Information Provided to the Senate Subcommittee and Published in the PSI Report

112. The record is clear that CUA failed to disclose certain crucial information to the Commission that CUA previously provided to the Senate Subcommittee and which was published in the PSI Report released on June 9, 2020. Specifically, CUA did not provide the Commission with relevant information concerning CUG's role {[ ]}[502] in CUA's management and operations, and failed to disclose a confidentiality agreement between CUG and CUA.[503] If the Commission were to consider only CUA's responses in the *Order to Show Cause*, the facts presented by CUA would suggest that CUG plays a very "innocuous role" in the management and operations of CUA.[504] However, the PSI Report, which cites to briefings given to Senate staff by representatives of CUA, demonstrates that CUA disclosed to the Subcommittee that CUG has a much broader role than was initially described to the Commission and later confirmed, in large part, by CUA in its response to the *Institution Order*.

113. *CUG's Role in CUA's Management and Operations*. In the *Order to Show Cause*, the Bureaus required CUA to provide a description of CUA's ownership and control (direct and indirect) and directed CUA to provide "a detailed description of its corporate governance."[505] On June 1, 2020, in its response, CUA contended that it is not subject to the "exploitation, influence, or control of the Chinese

(Continued from previous page)
00040, SPC-New-20070112-00002, ITC-214-20020728-00361, ITC-214-20020724-00427) (ISPC Reclamation Letter).

[496] *Institution Order*, 36 FCC Rcd at 6353, 6356-57, paras. 49, 55.

[497] *Id.* at 6353, para. 49.

[498] *Id.*; *see supra* para. 100.

[499] *Institution Order*, 36 FCC Rcd at 6353, para. 49.

[500] *Id*.

[501] 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 . . . ." 47 USC § 151.

[502] CUA Response to *Institution Order*, Business Confidential Exh. 3.

[503] *See* PSI Report at 49; *Institution Order*, 36 FCC Rcd at 6353-55, paras. 50-51.

[504] *Institution Order*, 36 FCC Rcd at 6353-54, para. 50.

[505] *Order to Show Cause*, 35 FCC Rcd at 3725, para. 9.

government . . . ."[506] To support this argument, CUA stated that it "is a distinct, separate legal entity that is subject to—and has complied with—U.S. laws and regulations."[507] CUA also provided a summary of its bylaws, and stated that CUG, its direct parent entity, "just like the common practices of other multinational companies alike, appoints the board members and management team, and approves the annual business plan and budget of CUA."[508]

114. Based on the PSI Report, it is clear that CUA's responses to the Bureaus' *Order to Show Cause* omitted crucial information that CUA provided to the Senate Subcommittee regarding CUG's role in and control over the management and operations of CUA.[509] Specifically, the information that CUA offered to the Senate Subcommittee concerning CUG's management and storage of CUA's customer records, monitoring of CUA's network operations, and provision of technical support, show CUG's high level of involvement in CUA's management and control.[510] As indicated in the *Institution Order*, the PSI Report states that CUG "manages CUA's U.S. customer records," and that "customer records are stored on servers in Hong Kong and maintained by CUG."[511] This is in opposition to CUA's response to the *Order to Show Cause*, which did not provide any details about CUG's role in CUA's corporate governance beyond the statement that CUG appoints CUA's board members and management team and approves CUA's annual business plan and budget.[512] The PSI Report further states that "[a]ccess to U.S. records is governed by [a confidentiality agreement], which includes requiring those seeking access to have a business justification; however, CUA representatives suggested that CUG decides what constitutes a sufficient justification."[513] CUA also informed the Senate Subcommittee that CUG monitors CUA's network operations, and CUA utilizes CUG's NOC in Hong Kong for technical support.[514] CUA informed the Senate Subcommittee, but not the Commission, that CUG can remotely configure CUA's network equipment.[515] Importantly, CUA failed to disclose all of this information to the Commission,[516] even though such information is directly relevant to the direction in the *Order to Show Cause* to provide "a description of [CUA's] ownership and control (direct and indirect)" and "'a detailed description of its corporate governance.'"[517] In its response to the *Institution Order*, CUA reiterates its arguments concerning CUA's independence from CUG, but admits that CUG has certain authority over CUA's management and control.[518]

---

[506] CUA Response to *Order to Show Cause* at 30.

[507] CUA Response to Executive Branch Letter at 12.

[508] CUA Response to *Order to Show Cause* at 20.

[509] *See Institution Order*, 36 FCC Rcd at 6354-55, para. 51; PSI Report at 78-79.

[510] *See* PSI Report at 78-79.

[511] PSI Report at 79 (citing Briefing with China Unicom Americas (Apr. 16, 2020)); *Institution Order*, 36 FCC Rcd at 6354, para. 50 (citing PSI Report at 79).

[512] CUA Response to *Order to Show Cause* at 20.

[513] PSI Report at 79 (citing Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee); Briefing with China Unicom Americas (Apr. 16, 2020)). CUA characterized this arrangement as "'common among international carriers.'" *Id.* (citing Briefing with China Unicom Americas (Apr. 16, 2020)); *Institution Order*, 36 FCC Rcd at 6354, para. 50.

[514] PSI Report at 79 (citing Briefing with China Unicom Americas (Apr. 16, 2020)); *Institution Order*, 36 FCC Rcd at 6354, para. 50 (citing PSI Report at 79).

[515] PSI Report at 79 (citing Letter from Squire Patton Boggs, counsel to CUA, to the Subcommittee (Apr. 29, 2020) (on file with the Subcommittee)); *Institution Order*, 36 FCC Rcd at 6354, para. 50 (citing PSI Report at 79).

[516] *See Institution Order*, 36 FCC Rcd at 6353-54, para. 50 (citing PSI Report at 79).

[517] *Id.* at 6353, para. 50 (quoting *Order to Show Cause*, 35 FCC Rcd at 3725, para. 9).

[518] *See supra* para. 55; CUA Response to *Institution Order* at 33-35.

115. *CUA/CUG Confidentiality Agreement*. CUA also failed to disclose to the Commission the existence of a confidentiality agreement between CUA and CUG {[ ]}[519] that "'governs access to the records and also establishes procedures to protect [CPNI].'"[520] As we stated in the *Institution Order*, based on how the PSI Report described the confidentiality agreement, the Commission "would have expected [CUA] to inform the Commission of the confidentiality agreement, particularly because it governs access to U.S. customer records," and the PSI Report indicates that CUG, not CUA, "controls access to U.S. customer records."[521] Further, upon consideration of CUA's response to the *Institution Order*, we affirm our preliminary view that the confidentiality agreement is a significant part of the management and control of CUA, and CUA should have disclosed it to the Commission in response to the *Order to Show Cause*.[522]

116. After CUA provided the confidentiality agreement in response to the Commission's request in the *Institution Order*,[523] our independent review of this document indicates that the confidentiality agreement is {[ ]}[524] CUA's response to the *Institution Order* provides no explanation as to why CUA represented to the Commission and the Senate Subcommittee that {[ ]}[526] Further, CUA's response to the *Institution Order* {[ ]} Despite CUA's assertion that it has

[519] CUA Response to *Institution Order*, Business Confidential Exh. 3; *see infra* para. 116.

[520] *Institution Order*, 36 FCC Rcd at 6354, para. 51 (quoting PSI Report at 79).

[521] *Id*.

[522] *See id*. at 6354-55, para. 51.

[523] *See Institution Order*, 36 FCC Rcd at 6362-32, Appx. A.

[524] CUA Response to *Institution Order*, Business Confidential Exh. 3 at 3 (stating that {[ ]}).

[525] *See, e.g.*, *id.*, Business Confidential Exh. 3 at 2 ({[ ]}); PSI Report at 79 ("CUA and CUG have signed a confidentiality agreement that governs access to the records and also establishes procedures to protect [CPNI]." (citing Briefing with China Unicom Americas (Apr. 16, 2020); Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee)).

[526] CUA Response to *Institution Order*, Business Confidential Exh. 3 at 2.

[527] *Id*. at 1-2.

[528] *Id*.

"corrected the factual record," the record reflects that CUA has not accurately described {[

]}[529]

117. CUA contends that its failure to provide information in response to the *Order to Show Cause* does not support a finding that CUA is untrustworthy,[530] because "[t]he Commission clearly had access to the information that CUA provided to the Senate Subcommittee, which was part of the Subcommittee's public report,"[531] and "any alleged discrepancies or omissions in CUA's responses to the [*Order to Show Cause*] were likely the product of CUA receiving different requests for information with different verbiage from different parties (the Commission and the Senate Subcommittee)."[532] CUA argues that, in any event, "any alleged unintended incomplete response is not sufficient justification for revocation of CUA's section 214 authorizations."[533] With respect to "the existence of a confidentiality agreement between CUA and [CUG]," CUA further argues that "[i]t is unfair for the Commission to assume that CUA should have interpreted either question as soliciting information about the confidentiality agreement."[534]

118. We find wholly unpersuasive CUA's contention that by "provid[ing] the 'omitted' or 'discrepant' information in question to another U.S. government entity – the Senate Subcommittee, [CUA] effectively ma[de] that information available to the Commission as well."[535] This argument ignores the fact that CUA was obligated in the first instance to provide complete and accurate responses to the Bureaus' inquiry in the *Order to Show Cause*. Additionally, although the PSI Report is publicly available, the underlying information upon which the Senate Subcommittee relied to reach its conclusions, such as correspondence with CUA and any supplementary documents provided to the Senate Subcommittee by CUA, is not in the public record. Indeed, we find it unreasonable for CUA to expect the Commission to seek information from another branch of government regarding matters between CUA and the Commission. Nor did CUA indicate after filing its response to the *Order to Show Cause* that

[529] *Id*.

[530] CUA argues that "the Commission attempts to paint CUA as untrustworthy by using CUA's June 1, 2020 responses to specific inquiries posed by the Commission in its Order to Show Cause." *Id.* at 18. CUA contends that "more than nine months after receiving CUA's responses, and without reverting to CUA in the meantime to seek additional information or clarification, the Commission claims that CUA's responses raise 'significant concerns.'" *Id.* (citing *Institution* Order, 36 FCC Rcd at 6353, para. 49).

[531] CUA Response to *Institution Order* at 18. CUA contends that this undercuts the Commission's argument that CUA was "unwilling to provide the relevant information, or was deliberately trying to hide such information, when it had already supplied it to another U.S. government entity." *Id*. at 18-19.

[532] *Id.* at 19.

[533] *Id*. at 20 (citing *BMW of North America, Inc. v. Gore*, 517 U.S. 559 (1996)); *see supra* para. 45 & note 187. CUA argues that, "[g]enerally, section 214 authorizations have been revoked when egregious, non-compliant conduct has occurred." CUA Response to *Institution Order* at 20. CUA claims that "[a]ny alleged discrepancies or omissions were not due to CUA's unwillingness to provide such information, and do not provide a basis for revoking CUA's section 214 authorizations." *Id*. at 21.

[534] CUA Response to *Institution Order* at 19 ("The Commission claims that CUA should have provided this information in response to the sixteen inquiries posed by the Commission, specifically in response to the requests seeking 'a description of the ownership and control of its direct and indirect owners, or in response to [its] . . . question asking for a "detailed description of [CUA's]… corporate governance."'") (citing *Institution Order*, 36 FCC Rcd at 6354, para. 51).

[535] CUA Response to *Institution Order* at 42.

further information relevant to this proceeding was contained in the PSI Report. We are similarly unpersuaded by CUA's argument that "any alleged discrepancies or omissions in CUA's responses to the [*Order to Show Cause*] were likely the product of CUA receiving different requests for information with different verbiage from different parties."[536] While it is unsurprising for the Commission and the Senate Subcommittee to ask CUA for information in different ways, we nevertheless expected CUA to provide us with complete responses to the questions posed in the *Order to Show Cause*. In that regard, the *Institution Order* required CUA to explain with specificity any discrepancies between the information that it submitted to the Commission and the information that it submitted to the Senate Subcommittee. CUA failed to do so and its responses to the *Institution Order* again provide additional evidence that CUA cannot be trusted to comply with the Commission's rules, provide truthful and accurate responses, and work cooperatively with the U.S. government generally.

b. Failure to Fully Respond to the *Order to Show Cause* and the *Institution Order*

119. *Indirect Controlling Interest Holders.* CUA also "did not provide the Commission with a full and accurate description of its indirect controlling interest holders, as directed by the *Order to Show Cause*."[537] The record therefore raised confusion as to the ownership and control of certain companies that share common ownership or are affiliated with CUA, including CU A-Share and China Unicom (BVI) Limited.[538] In its response to the *Order to Show Cause*, CUA provided an ownership chart that reflected that CU "has an effective interest of approximately *52.1%* of [CUHK's] equity."[539] The Executive Branch agencies, however, reported to the Commission that CUHK's 2020 SEC Annual Report stated that "[CU] indirectly controlled an aggregate of approximately *79.9%* of our issued share capital as of April 15, 2020."[540] CUA's response to the *Order to Show Cause* did not identify whether any entity held a controlling interest in CU A-Share, a public company within CUHK's chain of ownership. This raised a question as to whether CU controlled CU A-Share, and therefore CU (BVI) Limited, which would account for the difference between CU's "controlling interest" of 79.9% and its equity interest of 52.1% in CUHK. The *Institution Order* also stated that CUA did not identify and provide certain details concerning all officers, directors, and senior managers of *all* entities holding a 10% or greater ownership interest in CUA and requested that CUA provide this information and therefore directed CUA to address this discrepancy.[541]

120. In its response to the *Institution Order*, CUA again failed to provide "a complete and detailed description of the current ownership and control of" CUA.[542] CUA did not explain the Chinese

[536] *Id.* at 19.

[537] *Institution Order*, 36 FCC Rcd at 6355, para. 52. Specifically, the *Order to Show Cause* directed CUA to provide "a detailed description of the current ownership and control (direct and indirect) of the company and the place of organization of each entity in the ownership structure." *Order to Show Cause*, 35 FCC Rcd at 3725, para. 9.

[538] See *Institution Order*, 36 FCC Rcd at 6355, para. 52.

[539] CUA Response to *Order to Show Cause* at 18 (emphasis added).

[540] Executive Branch Letter at 20, n.122 (quoting 2020 CUHK SEC Annual Report at 13) (emphasis added).

[541] *Institution Order*, 36 FCC Rcd at 6355-56, para. 53. CUA only provided this information for its direct parent CUG, and did not provide this information for CUHK and CU, both of which have a greater than 10% interest in CUA. With respect to CUA's failure to provide certain information about CUHK and CU's directors, we stated that "[a]lthough we believe the answers would not be dispositive of [CUA's] independence from its direct and indirect parent entities, the Chinese Communist Party, or the Chinese government, we again question why [CUA] did not provide the Commission with a full response regarding [CUA's] and its direct and indirect parent entities' affiliations with the Chinese Communist Party. *Id*. at 6355, para. 53.

[542] *Id.* at 6362, Appx. A (directing CUA to provide, among other things, "a complete and detailed description of the current ownership and control of [CUA], including a description of the equity interest and voting interest for any entity that holds a ten percent or greater direct or indirect interest in and/or controls [CUA]").

government's ownership of CU A-Share and China Unicom (BVI) Limited in such a manner as to clarify the control of these entities. Because CUHK's SEC filing reflects that CUHK is controlled by CU, we assume that CU A-Share is controlled by CU, and therefore, the Chinese government. Although the absence of this information does not disturb our determination that CUA is ultimately owned and controlled by the Chinese government through various intermediary companies—as we infer CU's control of CUHK due to its equity interest, which is greater than 50%—CUA's failure to fully respond to the Commission's request demonstrates a lack of transparency, affecting our ability to trust the reliability of CUA's filings.[543] CUA also failed to explain the discrepancy between the information submitted in its response to the *Order to Show Cause* and the information that CUHK filed with the SEC.

c. Failure to Comply with the Commission's Rules

121. *Failure to Comply with ISPC Assignment Rules and Conditions.* Based on our assessment of CUA's response to the *Order to Show Cause*, CUA disregarded its responsibilities to the Commission as a holder of ISPCs.[544] On March 10, 2021, the International Bureau found that CUA was not in compliance with the conditions of its provisional ISPC assignments, and reclaimed its three ISPC assignments.[545] CUA was not in compliance with the conditions of its ISPC assignments because it failed to notify the Commission that ISPC 3-194-2 had been transferred from China Netcom (USA) Operations Limited to China Unicom USA Corporation and that all three of its ISPC assignments (3-194-2, 3-195-0, and 3-199-2) were not in use.[546] CUA admits that ISPC assignment 3-199-2 has not been used since 2009 and states that it "does not have any records with respect to its use prior to 2009 due to personnel changes."[547] CUA's disregard of the Commission's ISPC rules and conditions of its ISPC assignments is particularly concerning because ISPCs are a scarce resource that are used, for example, by international SS7 gateways as addresses for routing domestic voice traffic to an international provider or for other services.[548]

122. *Failure to File Timely Pro Forma Notification.* The *Order to Show Cause* directed CUA to explain "whether certain *pro forma* transfer of control actions occurred between 2009 and 2017 concerning the subject international section 214 authorizations and whether [CUA] appropriately notified the Commission, as required by Commission rules."[549] In its response to the *Order to Show Cause*, CUA confirmed that "a pro forma notification filing was not submitted with FCC for an internal reorganization by which internal control of CUA was transferred from [CUHK] to its wholly-owned subsidiary Billion Express Investments Co., Ltd. ('Billion', a BVI incorporated company) on December 30, 2011."[550] In the

[543] *See supra* paras. 7, 52 & note 22.

[544] *See generally* ISPC Reclamation Letter.

[545] *Id*. at 1.

[546] *Id*.; *see id.* at 4, n.29 (stating that CUA also failed to update the Commission's ISPC records to reflect China Unicom USA Corporation's name change to China Unicom Americas with regard to ISPC 3-194-2 and 3-195-0, which became effective on August 31, 2009).

[547] CUA Response to *Order to Show Cause* at 26.

[548] *See China Telecom Americas Institution Order,* 35 FCC Rcd at 15040, para. 58 ("ISPCs are a scarce resource that are used by international [SS7] gateways as addresses for routing domestic voice traffic to an international provider and anyone seeking an ISPC assignment is required by rule to file an application with the Commission and comply with its procedures."); *Reporting Requirements for U.S. Providers of International Telecommunications Services Amendment of Part 43 of the Commission's Rules*, IB Docket No. 04-112, Notice of Proposed Rulemaking, 19 FCC Rcd 6460, 6474, para. 36, n.83 (2004).

[549] *Order to Show Cause*, 35 FCC Rcd at 3726, para. 9; *Institution Order*, 36 FCC Rcd at 6356, para. 55 (quoting *Order to Show Cause*, 35 FCC Rcd at 3726, para. 9).

[550] CUA Response to *Order to Show Cause* at 29; *see Institution Order*, 36 FCC Rcd at 6356, para. 55 (quoting CUA Response to *Order to Show Cause* at 29). CUA did, however, file a *pro forma* notification in 2017 after

(continued….)

Institution Order, we noted that CUA had not taken any steps to submit a separate filing to the Commission to clarify the ownership history of its section 214 authorizations, despite having been made aware of the failure to file a *pro forma* notification in the *Order to Show Cause* released on April 24, 2020.[551] In fact, in its response to the *Institution Order*, CUA did not mention its failure to file a *pro forma* notification concerning the 2011 reorganization beyond a brief mention in a footnote.[552] On September 8, 2021, CUA filed a *pro forma* notification for the 2011 reorganization, nearly a year and a half after the Bureaus first raised the question in the *Order to Show Cause*.[553] While we recognize, as stated by CUA, that "the reorganization did not result in a change in the actual or ultimate control of [CUA]," the Commission's rules nevertheless require all international section 214 authorization holders, including CUA, to ensure accurate corporate ownership is on file with the Commission and to submit any notifications of *pro forma* changes in control within thirty days pursuant to section 63.24(f).[554] At a minimum, given the significance of this proceeding, CUA should have taken corrective action to comply with the Commission's rules immediately upon being informed of its noncompliance on April 24, 2020. CUA's failure to do so evinces a disregard for Commission requirements and serves as additional evidence that CUA cannot be relied upon to comply with Commission rules.

123. Based on the record evidence, we find that the Commission, Executive Branch agencies, and other bodies within the U.S. government cannot trust CUA, particularly in light of the serious national security and law enforcement concerns associated with CUA's vulnerability to exploitation, influence, and control by the Chinese government. Additionally, CUA's omission of crucial information, failure to provide accurate and true statements to the Commission in response to the *Order to Show Cause* and *Institution Order*, and failure to comply with the Commission's rules provide evidence that CUA cannot be trusted. The trust, transparency, and reliability that are essential to an authorization holder's ability to comply with the Commission's statutory authority and implementing rules are simply not present with CUA. We reject CUA's arguments that "[a]ny alleged discrepancies or omissions were not due to CUA's unwillingness to provide such information, and do not provide a basis for revoking CUA's section 214 authorizations."[555] As we have already stated here and on several other occasions, the Commission has an "ongoing responsibility to evaluate all aspects of the public interest, including national security and law enforcement concerns that are 'independent of our competition analysis.'"[556] Independent of our concerns above, we separately revoke CUA's section 214 authority based on CUA's representations to the Commission and Congress to protect the national security and law enforcement

(Continued from previous page)
CUA's ownership was transferred from Billion to CUG and could have taken corrective action at that time to comply with Commission rules. *Institution Order*, 36 FCC Rcd at 6356, para. 55.

[551] *Institution Order*, 36 FCC Rcd at 6356, para. 55.

[552] *See* CUA Response to *Institution Order* at 20, n.90 (" . . . CUA hereby incorporates by reference its previous position that the failure to file a *pro forma* notification is not sufficient to justify revocation of its section 214 authorizations.").

[553] *Order to Show Cause*, 35 FCC Rcd at 3726, para. 9.

[554] *Institution Order*, 36 FCC Rcd at 6356, para. 55; 47 CFR § 63.24(f).

[555] CUA Response to *Institution Order* at 21. CUA also asserts that it "has always endeavored to engage fulsomely and candidly with the Commission, including in its response to the [*Order to Show Cause*]" and that "the Commission has unfairly imputed a nefarious motive to what it describes as 'discrepancies and/or omissions' in CUA's statements to the Commission and to the Senate Subcommittee." *Id.* at 42. We find here that irrespective of motive, CUA's responses to the questions posed in the *Order to Show Cause* and *Institution Order*, as described above, were opaque, inconsistent, and incomplete, which affirms our concerns regarding CUA's lack of candor, reliability, and trustworthiness.

[556] *China Telecom Americas Order on Revocation and Termination* at *6, para. 17 (quoting *China Telecom Americas Institution Order*, 35 FCC Rcd at 15016, para. 19 (citing *Foreign Participation Order*, 12 FCC Rcd at 23919, 23921, paras. 63, 65)).

interests of the United States. Given this finding, we find it unnecessary to address CUA's pending *pro forma* notification, and we therefore dismiss it as moot.[557]

C. Mitigation Would Not Address National Security and Law Enforcement Concerns

124. Based on the record, we find that mitigation would not address the significant national security and law enforcement concerns present in this case. We have a longstanding policy of according deference to the Executive Branch agencies' expertise in identifying and mitigating risks to national security and law enforcement interests.[558] The Executive Branch agencies, which have expertise in monitoring carriers' compliance with risk mitigation agreements, state that "[a]lthough concerns regarding the reliability of every telecommunications carrier must be evaluated when proposing mitigation measures," those concerns are magnified in this case "given CUA's relationship with the [Chinese] government and the significant national security and law enforcement concerns resulting from that relationship."[559] We agree with the Executive Branch agencies that, "because the underlying foundation of trust that is needed for a mitigation agreement of this type to adequately address national security and law enforcement concerns is not present, the opportunity for effective mitigation with CUA is illusory at best in the current national security environment."[560]

125. The Executive Branch agencies explain that "[d]ue to the sensitivity of national security and law enforcement investigations, the Executive Branch relies on a baseline level of trust when working with telecommunications carriers."[561] The Executive Branch agencies assert that, "[b]ecause CUA is ultimately owned by the [Chinese] government, the U.S. government cannot trust CUA to identify, disrupt, or provide assistance for investigations into unlawful activity sponsored by the [Chinese] government."[562] The Executive Branch agencies explain that CUA's relationship to the Chinese government impedes the U.S. government's ability to conduct statutorily authorized law enforcement and national security missions, and to protect information about targets and classified sources and missions.[563] The Executive Branch agencies assert that any breaches of a mitigation agreement by CUA, "even if promptly discovered and resolved, very likely cannot be remediated."[564]

---

[557] *See supra* para. 8.

[558] *See supra* para. 5; *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; *Institution Order*, 36 FCC Rcd at 6322, 6333, 6335-36, paras. 4, 23, 26.

[559] Executive Branch Letter at 37.

[560] *Id.* at 38 (citing *China Mobile USA Order*, 34 FCC Rcd at 3380, para. 38).

[561] *Id.* at 37. According to the Executive Branch agencies, "[e]ven with regular compliance monitoring, there can never be full visibility into all of the activities of a company, and there must be trust in order to rely on the other party to adhere rigorously and scrupulously to mitigation agreement provisions, and to self-report any problems of non-compliance." *Id.*

[562] *Id.*; *see id.* (stating, "because CUA is subject to exploitation, influence, and control by the [Chinese] government, CUA could—at the behest of that government, and as it may be required to do so under [Chinese] law—fail to self-report any violations of a mitigation agreement with the U.S. government"); *Institution Order*, 36 FCC Rcd at 6358, para. 58 (quoting Executive Branch Letter at 37).

[563] Executive Branch Letter at 36-37. The Executive Branch state that "the [Chinese] government's indirect ownership and control of CUA may result in particular conflicts of interest that could impair CUA's compliance with lawful U.S. process that seeks information transmitted using networks connected to China. In other instances, U.S. authorities may have particular sensitivities that could limit the sharing of information with CUA due to concerns that [CU] and other affiliates would become aware of U.S. authorities' interests in information related to CUA's services or [People's Republic of China]-related investigations." *Id.* at 36-37.

[564] *Id.* at 37; *Institution Order*, 36 FCC Rcd at 6358, para. 58. The Executive Branch agencies state that "disclosure to the [Chinese] government of national security or law enforcement requests, or the unauthorized access to customer or company data, could create irreparable damage to U.S. national security," and the Executive Branch

(continued….)

126. CUA, in response, indicates its lack of opportunity to negotiate a mitigation agreement to address national security and law enforcement concerns, stating that mitigation measures "are not without precedent" and "for more than two decades, the Commission, based on Letters of Assurance negotiated between carriers and the Department of Justice, has imposed conditions on numerous section 214 authorizations of foreign-owned carriers to address similar concerns."[565] CUA states that it "is willing and able to consider any proposed mitigations measures,"[566] and adds that it "provided details of proposed mitigation measures" in its response to the *Order to Show Cause*.[567] CUA contends that the Executive Branch agencies "engag[ed] in 'extensive discussions' with another telecommunications company that posed alleged national security and law enforcement concerns due to its potential control by the Chinese government," citing the *China Mobile USA* proceeding.[568] CUA indicates that it "has not been accused of any specific conduct jeopardizing U.S. national security and law enforcement interests, [and] is rebuffed without any discussions at all."[569] CUA adds that the Executive Branch agencies "had very limited time to conduct a meaningful analysis of potential mitigation measures in CUA's case"[570] and "[f]undamental fairness dictates that the Executive Branch agencies should explore less drastic measures prior to Commission revocation."[571]

(Continued from previous page)
would not be able to work effectively with CUA "to identify and disrupt unlawful activities such as computer intrusions, or to assist in the investigation of past and current unlawful conduct, as the U.S. government does with trusted voice communication providers." Executive Branch Letter at 37-38; *see id.* at 36; *Institution Order*, 36 FCC Rcd at 6358, para. 58 (citing Executive Branch Letter at 37-38).

[565] CUA Response to *Institution Order* at 28-29 & n.117 (citing *International Authorizations Granted*, 25 FCC Rcd 17052, 17053 (IB 2010); *China Mobile USA Order*, 34 FCC Rcd at 3371-72, para. 20, n.63 and quoting from the *China Mobile USA Order*, "'[w]e acknowledge that foreign government control of a U.S. carrier in and of itself is not grounds for denial of an international section 214 [application]. In fact, in keeping with the WTO commitments of the United States, the Commission has granted several such authorizations to entities with foreign government ownership.'") (omission by CUA of bracketed language); *see* CUA Response to *Order to Show Cause* at 9.

[566] CUA Response to *Institution Order* at 29.

[567] *Id.*; *see* CUA Response to *Order to Show Cause* at 15; CUA Response to *Order to Show Cause*, Business Confidential Exh. 1 (proposing {[

]}); *Institution Order*, 36 FCC Rcd at 6358, para. 59.

[568] CUA Response to *Institution Order* at 29 & n.120 (citing *China Mobile USA Order*, 34 FCC Rcd at 3365, n.26 and arguing, "that company did not even possess section 214 authorizations and therefore lacked CUA's established record of compliance"). *See id.*, n.120 ("In a separate proceeding involving another telecommunications company with purported vulnerabilities to the Chinese government, the Executive Branch agencies 'exchanged correspondence and participated in [tele]conferences and meetings . . . on at least 90 occasions.'") (citing China Telecom (Americas) Corporation, Response to Order to Show Cause, GN Docket No. 20-109 (June 8, 2020), Exh. 16) (omission by CUA of bracketed language).

[569] *Id.* at 29.

[570] *Id.* at 29-30. *See supra* note 145.

[571] *Id.* at iii; *see id.* (contending, "even if there arguably were potential legitimate national security or law enforcement concerns, there are alternatives to the draconian remedy of revocation that never have been explored with CUA despite its offer to do so"); *id.* at 29; CUA Response to *Order to Show Cause* at 15 (arguing, "fundamental fairness dictates that the Commission should explore less drastic measures prior to any revocation").

127. CUA presents no additional evidence or arguments in its response to the *Institution Order* that convince us that mitigation would be appropriate or adequate to address the national security and law enforcement risks identified by the Executive Branch agencies. As we indicated in the *Institution Order*, we are not persuaded by CUA's arguments given the serious national security and law enforcement risks identified in the record.[572] CUA fails to persuasively explain how the substantial and unacceptable concerns surrounding CUA's ownership, access of its records by non-U.S. affiliates, and its vulnerability to exploitation, influence, and control by the Chinese government could be ameliorated notwithstanding the Executive Branch agencies' assertion that mitigation would not be feasible in this instance. Moreover, CUA disagrees with our fundamental concerns in this proceeding—namely, concerns over CUA's ownership and control by the Chinese government raising substantial and unacceptable national security and law enforcement risks—and therefore assumes that there are workable mitigation measures.[573]

128. We also reject CUA's contentions that "the record fails to show how [the Executive Branch agencies] have even seriously considered and evaluated" mitigation measures[574] and that the Executive Branch agencies raise "conclusory assertions."[575] Contrary to CUA's suggestion, the Commission adopted procedures in the *Institution Order* that allowed for CUA, interested Executive Branch agencies, and the public to present further arguments or evidence in this matter.[576] In fact, the Executive Branch agencies advise in their letter that the national security and law enforcement risks that they identify concerning CUA "will come as no surprise to the [Commission], as the same risks were applicable and were identified in detail in the recommendation submitted to the [Commission] concerning [China Telecom Americas'] international Section 214 authorizations."[577] The Executive Branch agencies did not ask the Commission for more time to consider mitigation with CUA and instead stated that "[b]ased on the concerns articulated [in the Executive Branch Letter], as well as those identified in the recommendations for [China Telecom Americas] and [China Mobile USA], both similarly situated companies, it does not appear that a mitigation agreement with CUA would be feasible."[578] We find nothing in the record to support CUA's arguments.

129. We find that the record reflecting the national security and law enforcement risks that the Executive Branch agencies identified with regard to CUA's vulnerability to the exploitation, influence, and control of the Chinese government, raises serious concerns as to whether CUA can be trusted to cooperate with the Executive Branch agencies' mitigation monitoring in good faith and with transparency, and to comply with mitigation terms.[579] Finally, given the evidence in the record demonstrating CUA's lack of transparency and reliability in its dealings with the Commission, we agree with the Executive Branch agencies that CUA is not likely to cooperate and be fully transparent with the Executive Branch agencies in such a way that would allow a mitigation agreement to be effective.[580]

---

[572] *See Institution Order*, 36 FCC Rcd at 6357-59, para. 57-60.

[573] *See, e.g.*, CUA Response to *Institution Order* at 22-26, 36-40; CUA Response to *Order to Show Cause* at 9-11, 29-33. *But see Institution Order*, 36 FCC Rcd at 6334-53, 6357-59, paras. 24-48, 57-60.

[574] CUA Response to *Institution Order* at iii.

[575] *Id.* at 29 (arguing that CUA "must defend itself against conclusory assertions that mitigation measures cannot resolve national security and law enforcement concerns").

[576] *Institution Order*, 36 FCC Rcd at 6319-20, 6359, 6360, paras. 1, 61, 66.

[577] Executive Branch Letter at 2 (citing Executive Branch CTA Recommendation at 1).

[578] *Id.* at 38.

[579] *See generally* Executive Branch Letter; *Institution Order*, 36 FCC Rcd at 6357-59, para. 57-60.

[580] *See supra* Section III.B.3.; *Institution Order*, 36 FCC Rcd at 6359, para. 60.

D. Transition Period

130. We direct CUA to discontinue all services provided under section 214 authority no later than sixty (60) days from the release date of this Order. We require CUA to provide all affected customers with thirty (30) days' notice of service discontinuance. Such notice shall be in writing to all affected customers, except MVNO customers. CUA must notify its MVNO customers either by providing written notice or by text message to their mobile number. In its letter or notification to its MVNO customers, CUA must certify its compliance with this requirement. We further require CUA to file a copy of the standard notice(s) sent to its customers (without providing the Commission with any customer PII information) in the docket of this proceeding through the Commission's Electronic Comment Filing System (ECFS) and the relevant file numbers in the International Bureau Filing System (IBFS) within sixty (60) days of release of this Order.[581]

131. We reject CUA's request to grant it a transition period of at least {[ ]} to discontinue its services provided pursuant to section 214.[582] In the *Institution Order*, we asked CUA to provide "a complete description of all work required for China Unicom Americas to discontinue all section 214 services to its customers if the Commission were to revoke China Unicom Americas' section 214 authority, along with a detailed estimate of the time required for each portion of that work and an explanation of how that estimate was reached."[583] In its response, CUA states that there are {[

[581] CUA should follow the procedures set out in this *Order* rather than those in section 63.71 of the Commission's rules. 47 CFR § 63.71.

[582] CUA Response to *Institution Order*, Business Confidential Exh. 6.

[583] *Institution Order*, 36 FCC Rcd at 6363, Appx. A.

[584] CUA Response to *Institution Order*, Business Confidential Exh. 6 at 1.

[585] *Id.* at 2.

[586] *Id.*

[587] *Id.* at 2-3.

[588] *Id.* at 2. {

]}

[589] *Id.* at 3.

]}[590]

132. As we described in the *China Telecom Americas Order on Revocation and Termination*, the Commission's relevant discontinuance rules for international services generally provide for a 30-day transition period.[591] For domestic services, the discontinuance rules provide for a 31-day transition period from the date an application is accepted for filing provided by a carrier, such as CUA, that does not have market power in the United States, and a 60-day transition period from the date an application is accepted for filing provided by a carrier found to have market power in the United States.[592] CUA has not demonstrated that its customers would be unable to obtain an adequate replacement service provider or that its customers need a longer time period to transition to another service provider. {[

]} Based on the record, however, CUA provides its MVNO service as a prepaid service without a contract.[593] As for its enterprise customers, {[

]}[596]

133. As we found in the *China Telecom Americas Order on Revocation and Termination*,[597] a 60-day transition period providing no less than 30 days' notice to customers is appropriate and should mitigate any difficulties CUA's customers may face in finding other providers that offer Chinese-

[590] *Id.*

[591] *China Telecom Americas Order on Revocation and Termination* at *52, para. 154. *See* 47 CFR § 63.19.

[592] *China Telecom Americas Order on Revocation and Termination* at *52, para. 154. *See* 47 CFR § 63.71(f)(1).

[593] CUA Response to *Order to Show Cause*, Business Confidential Exh. 6 at 3; CUA Response to *Order to Show Cause* at 46.

[594] CUA Response to *Order to Show Cause*, Business Confidential Exh. 6, Attach. 6-A.

[595] *See* Information & Resources: China Telecom (Americas) Can No Longer Provide Mobile Service in the United States; CTExcel Customers Need to Switch to a New Service Provider by January 3, 2022 (*CTA Consumer Guide*) (available at https://www.fcc.gov/consumers/guides/information-and-resources-china-telecom-americas-can-no-longer-provide-mobile).

[596] CUA Response to *Order to Show Cause*, Business Confidential Exh. 6, Att. 6-A; *see also supra* Sections III.B, III.C.

[597] *China Telecom Americas Order on Revocation and Termination* at *52, para. 154.

language customer support.[598] We also note that this proceeding was initiated almost two years ago, providing customers with notice that CUA might have its section 214 authority revoked and have to discontinue its services provided under that authority.

134. We recognize that U.S. customers generally have many low-cost options for international calls, including to China, and at least some of these options offer Chinese-language support. As we did when we revoked and terminated China Telecom Americas' section 214 authority,[599] upon release of this Order, we will seek to raise consumer awareness by issuing a consumer guide in English, Simplified Chinese, and Traditional Chinese on the Commission's website, advising CUA's MVNO customers of our decision and raising awareness of other options for mobile service.

IV. ORDERING CLAUSES

135. Accordingly, IT IS ORDERED, pursuant to sections 1, 4(i), 4(j), 214, 215, 218, and 403 of the Communications Act of 1934, as amended, 47 U.S.C. §§ 151, 154(i), 154(j), 214, 215, 218, 403, and section 1.1 of the Commission's rules, 47 CFR § 1.1, that China Unicom (Americas) Operations Limited's domestic section 214 authority and international section 214 authorizations are REVOKED.

136. IT IS FURTHER ORDERED that China Unicom (Americas) Operations Limited must discontinue all services provided pursuant to section 214 authority no later than sixty (60) days from the release date of this Order.

137. IT IS FURTHER ORDERED that the *pro forma* transfer of control notification filed by China Unicom (Americas) Operations Limited IS DISMISSED AS MOOT.

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

China Unicom (Americas) Operations Limited
c/o Robert E. Stup, Jr.
Paul C. Besozzi
Rebecca A. Worthington
Caroline Howard
Squire Patton Boggs (US) LLP
2550 M Street NW
Washington, DC 20037

[598] One factor the Commission considers in determining whether to authorize a carrier to discontinue service is the adequacy of available replacement services. *See Verizon Telephone Companies Section 63.71 Application to Discontinue Expanded Interconnection Service Through Physical Collocation*, Order, 18 FCC Rcd 22737, 22742, para. 8 (2003); *Technology Transitions et al.*, Declaratory Ruling, Second Report and Order, and Order on Reconsideration, 31 FCC Rcd 8283, 8303-04, paras. 61-62 (2016).

[599] *China Telecom Americas Order on Revocation and Termination* at *53, para. 155. *See* Letter from Patrick Webre, Chief, Consumer and Governmental Affairs Bureau, Thomas Sullivan, Chief, International Bureau, and Kris Monteith, Chief, Wireline Competition Bureau to Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP (dated Nov. 12, 2021) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285) (The Commission disagreed with CTA that releasing a consumer guide would be misleading or disruptive to CTA's customers. The Commission noted that the release of the consumer guide does not preclude CTA from issuing its own communications to its customers.) *See also CTA Consumer Guide*, *supra* note 595.

Tong Zhang, CEO
China Unicom (Americas) Operations Limited
2355 Dulles Corner Blvd, Suite 688
Herndon, VA 20171

Wesley Haiqiang Liu, Associate President
China Unicom (Americas) Operations Limited
2355 Dulles Corner Blvd, Suite 688
Herndon, VA 20171

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

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, ITC-214-20020728-00361; ITC-214-20020724-00427

Today we take another critical step to protect our communications networks from foreign national security threats. We direct China Unicom Americas to discontinue any domestic or international services that it provides pursuant to its section 214 authority.

We reach this decision carefully. To understand why requires a bit of history.

It was more than two decades ago that China Unicom Americas first received section 214 authorization from the Federal Communications Commission to provide domestic and international service in the United States. But since that time, the national security landscape has shifted and there has been mounting evidence—and with it, a growing concern—that Chinese state-owned carriers pose a real threat to the security of our telecommunications networks.

As a result, in 2019, the Commission denied China Mobile USA the authority to enter the United States market for national security reasons. In 2020, the Senate Permanent Subcommittee on Investigations issued a report on the threats associated with Chinese state-owned carriers operating in the United States.

At roughly the same time, the FCC took steps to consider the threat posed by China Unicom Americas. That's because China Unicom Americas shares the characteristics highlighted by our national security agencies with respect to China Mobile USA. Accordingly, the International Bureau, the Enforcement Bureau, and the Wireline Competition Bureau issued an Order to Show Cause to China Unicom Americas that directed the company to demonstrate why the agency should not initiate a proceeding to revoke its domestic and international section 214 authority.

Once China Unicom Americas responded, the FCC reached out to its national security partners for their perspective and expertise. We asked the Department of Justice, on behalf of the Attorney General, to address the arguments made by China Unicom Americas in its response to the Order to Show Cause. The Executive Branch, represented by NTIA, responded to the letter and provided their view that China Unicom Americas was subject to the control of the Chinese Government.

At each stage in the process, China Unicom Americas had an opportunity to respond. And at each stage, China Unicom Americas' responses were incomplete, misleading, or incorrect.

As a result, last year we found that China Unicom Americas failed to dispel those concerns regarding the retention of its authority to provide telecommunications services in the United States. And we provided China Unicom Americas another opportunity to make its case. We also sought additional guidance from our partners in the Executive Branch before reaching our decision today.

On the basis of this record, we believe it is clear that the public interest is no longer served by China Unicom Americas' retention of its section 214 authority. So we revoke China Unicom Americas' domestic and international section 214 authority and direct China Unicom Americas to discontinue within 60 days of the release of this order any domestic or international services that it provides pursuant to this authority.

Of course, this isn't the first time we've taken action to withdraw section 214 authority to protect our communications infrastructure from the threat posed by Chinese state-owned carriers. In 2021, we revoked China Telecom Americas' prior authorization to provide service within the United States. We also have started similar revocation proceedings against two other companies, Pacific Networks Corp. and ComNet (USA) LLC.

Today's action is the latest in a series of steps we've taken to keep our networks secure. In the last year, we have pursued a multi-faced approach to protect communications and strengthen our national security.

We are making our supply chains more transparent. In March of last year, the FCC published the first-ever list of communications equipment and services that pose an unacceptable risk to national security. This is known as the Covered List. Congress gave our national security and law enforcement agencies the primary responsibility to determine what equipment and services should be added to this list over time. So this month I sent letters to the Department of Commerce, the Office of the Director of National Intelligence, the Federal Acquisition Security Council, the Department of Justice, and the Federal Bureau of Investigation so that we can update the Covered List by March of this year. That means we will very shortly confirm the status of other companies that have been the subject of recent security attention. But it's not enough to know what the risk is, we need to know where it is, too. So we are also getting ready to launch a new data collection under the Secure and Trusted Communications Networks Act that will require providers to report whether or not they have equipment or services on the Covered List.

We are locking down our universal service programs. We've prohibited the use of funds from these programs to purchase equipment on our Covered List.

We are replacing insecure equipment in our networks. In October, we launched a $1.9 billion program to remove equipment from Huawei and ZTE to the extent that it is present in our domestic networks today. In doing so, we created opportunities to transition to Open RAN systems, which will help diversify the technology in our networks and support a market for more secure 5G equipment.

We are reviewing submarine cables with greater care. We have worked with the Department of State to change the 20-year-old process used for approving licenses for submarine cables. The revised approach better incorporates the new Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector into the assessment process. There will be no rubber-stamping applications. Instead, we have careful review.

We are updating our equipment authorization process. We have proposed rules that will align our equipment authorization procedures with our national security policies and ensure that going forward the FCC will not approve equipment from any companies on the Covered List.

We are reducing cyber risk. In light of recent data breaches, we have proposed stricter data breach reporting rules. We have launched a Notice of Inquiry on security of the Internet of Things. And we are rechartering the Cybersecurity Regulators Forum that has been dormant for the past few years—and assuming its leadership.

We are keeping 5G security front of mind and working with new partners to do so. We rechartered the Communications, Security, Reliability, and Interoperability Council and gave it a 5G focus. And for the first time, CSRIC is being co-chaired by the Cybersecurity and Infrastructure Security Agency—so we have a whole-of-government approach to 5G security.

These initiatives cut across the work of the agency. That's not an accident. Last year, I established the National Security Policy Committee, a dedicated, cross-bureau team of experts advancing a comprehensive approach to security matters at the FCC. The work they've done in the last year is thoughtful and impressive—and there's more to come.

Thank you to the staff who worked on today's decision, including Denise Coca, Kate Collins, Francis Gutierrez, Jocelyn Jezierny, Gabrielle Kim, David Krech, Wayne Leighton, Tom Sullivan, and Troy Tanner from the International Bureau; Eduard Bartholme, Michael Snyder, Mark Stone, and Patrick Webre from the Consumer and Governmental Affairs Bureau; Jeffrey Gee, Rosemary Harold, Pam Kane, and Christopher Killion from the Enforcement Bureau; Bob Cannon, Catherine Matraves, Deena Shetler, Emily Talaga, and Virginia Metallo from the Office of Economics and Analytics; Padma Krishnaswamy from the Office of Engineering and Technology; Ken Carlberg, Lisa Fowlkes, Jeffery Goldthorp, Deb Jordan, and Nicole McGinnis from the Public Safety and Homeland Security Bureau; Pam Arluk, Michele Berlove, Melissa Droller Kirkel, Jodie May, Rodney McDonald, Kris Monteith, and Terri Natoli from the Wireline Competition Bureau; Garnet Hanly and Susannah Larson from the Wireless Telecommunications Bureau; and Matthew Dunne, Michele Ellison, Doug Klein, Jacob Lewis, Scott Noveck, Bill Richardson, Joel Rabinovitz, and Royce Sherlock from the Office of General Counsel.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, ITC-214-20020728-00361; ITC-214-20020724-00427

In 2019, when we blocked China Mobile USA from entering the U.S. market based on national security concerns, I said it was time for a top to bottom review of every telecom carrier with ties to the communist regime in China. Many of these firms were authorized to operate in the U.S. decades ago and the potential security threats have evolved substantially in the intervening years. With that type of review in mind, the FCC opened investigations into several carriers—including the carrier at issue here, China Unicom Americas.

Consistent with the actions the Commission took against China Mobile USA in 2019 and China Telecom Americas in 2021, our decision today is informed by the views submitted by the Executive Branch agencies with responsibility for national security reviews. As our record here shows, those agencies have advised the FCC that there are serious national security and law enforcement risks associated with China Unicom Americas' continued access to U.S. telecommunications infrastructure. They also stated that China Unicom Americas' operations provide opportunities for Chinese state-sponsored actors to engage in economic espionage and other forms of theft of high value U.S. targets, including businesses and government agencies. Indeed, the FCC's own review found that China Unicom Americas poses significant national security concerns due to its control and ownership by the Chinese government, including its susceptibility to complying with Communist China's intelligence and cybersecurity laws. Our review also found that China Unicom Americas' conduct towards the Commission and Congress lacked candor and trustworthiness. Together, these factors present an unacceptable risk to our national security and therefore I support today's decision.

The threat to our networks from entities aligned with Communist China is one that we must address head on, and I am pleased that the FCC continues to show the strength and resolve necessary to meet this challenge. But as the threat landscape evolves, so too must our response. Fortunately, Congress granted us with tools—including the Covered List—to keep America's networks secure. Our determination that China Unicom Americas presents an unacceptable national security risk appears sufficient to trigger the process of adding them to our Covered List. Doing so could impose additional restrictions on China Unicom Americas that go beyond the scope of our section 214 authorizations, so I encourage the Commission to take appropriate action on this front, as I have recommended with China Telecom Americas before.

I look forward to continuing to work with my FCC colleagues on ways to protect America's communications networks and, in turn, our national security. My sincere thanks to the staff who prepared today's item. It has my support.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *China Unicom (Americas) Operations Limited*, GN Docket No. 20-110, ITC-214-20020728-00361; ITC-214-20020724-00427

From the basic convenience of wireless calling to the promise of the metaverse, advanced communications and information service technologies are transforming every aspect of our lives. 5G and other advanced broadband technologies are shifting into a new gear, and the race for 6G is already well underway.

But one byproduct of universal, always-on connectivity is the potential vulnerability it creates. As our networks connect with others around the world, we will inevitably encounter bad actors. We must remain on guard against any efforts to intercept, tamper with, or block our communications.

Today's decision is the latest in a series of FCC actions against such threats, and I fully support it. As our order states, the evidence clearly establishes that China Unicom Americas is subject to the exploitation, influence, and control of the Chinese government. As such, the company is highly likely to be forced to comply with Chinese government requests – including the disclosure of communications by American citizens – without sufficient legal protections and independent judicial oversight. Moreover, the company's actions during this investigation, including its failure to provide accurate and truthful information to the Commission, further demonstrate that China Unicom Americas simply cannot be trusted to provide telecommunications service in the United States. Our decision to revoke the company's authority to provide such service makes us more secure.

But there is more work to do. For example, data centers have become critical parts of the American communications and technologies sectors and are instrumental to new use cases like edge computing. As I've noted previously, however, even after loss of their section 214 authority, companies like China Unicom Americas can continue to offer data center services to American customers. The Department of Homeland Security has warned that these data centers leave their customers vulnerable to data theft for one of the same reasons underlying our decision today – these companies are legally required to secretly share data with the Chinese government or other entities upon request, even if that request is illegal under U.S. law. While the FCC currently lacks jurisdiction to address this potential national security threat, we should work with the Administration and Congress to examine whether the Commission needs broader authority to tackle this and other network security threats.

Thank you to the staff of the International Bureau for their work on this item.