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

In the Matter of	)	
	)	
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

Adopted: October 26, 2021 **Released: November 2, 2021**

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

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION

1. In this Order on Revocation and Termination (Order), we revoke China Telecom (Americas) Corporation's (CTA) domestic authority and revoke and terminate its international authority, pursuant to section 214 of the Communications Act of 1934, as amended (Act).[1] Based on our public

[1] 47 U.S.C. § 214; *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 to Show Cause, 35 FCC Rcd 3713 (IB, WCB, (continued….)

interest analysis under section 214 of the Act and the totality of the extensive unclassified record alone, we find that the present and future public interest, convenience, and necessity is no longer served by CTA's retention of its section 214 authority.

2. First, we find that CTA, 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 CTA to provide telecommunications services in the United States, we find that CTA's ownership and control by the Chinese government raise significant national security and law enforcement risks by providing opportunities for CTA, its parent entities, and the Chinese government to access, store, disrupt, and/or misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States. Third, independent of these concerns, CTA's conduct and representations to the Commission and other U.S. government agencies 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 further mitigation would not address these significant national security and law enforcement concerns. We therefore revoke CTA's domestic and international section 214 authority. Fifth, separate and apart from our findings concerning revocation, we terminate CTA's international section 214 authorizations based on CTA's willful violation of two of the five provisions of the 2007 Letter of Assurances[2] with the Executive Branch agencies, compliance with which is an express condition of its international section 214 authorizations.[3] Finally, although it is not necessary to support these findings and conclusions, we find that the classified evidence submitted by the Executive Branch agencies[4] further

(Continued from previous page)
EB 2020) (*Order to Show Cause*); *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) (*Institution Order*); China Telecom (Americas) Corporation, Response of China Telecom (Americas) Corporation to Order to Show Cause, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (June 8, 2020) (CTA June 8, 2020 Response) (filing with the Commission a public filing and a non-public business confidential filing); China Telecom (Americas) Corporation, Reply Comments of China Telecom (Americas) Corporation to Order Instituting Proceedings, GN Docket No. 20-109 (Mar. 1, 2021) (CTA Mar. 1, 2021 Reply).

[2] Department of Homeland Security, Department of Justice, Federal Bureau of Investigation, Petition to Adopt Conditions to Authorizations and Licenses, File No. ITC-T/C-20070725-00285, at 1 (filed Aug. 9, 2007) (Petition to Adopt Conditions to Authorizations and Licenses); Letter from Yi-jun Tan, President, China Telecom (USA) Corporation, to Sigal P. Mandelker, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Elaine N. Lammert, Deputy General Counsel, Federal Bureau of Investigation, and Stewart A. Baker, Assistant Secretary for Policy, U.S. Department of Homeland Security (July 17, 2007) (on file in ITC-T/C-20070725-00285) (2007 LOA).

[3] Under section 214(c) of the Act, the Commission "may attach to the issuance of the certificate such terms and conditions as in its judgment the public convenience and necessity may require." 47 U.S.C. § 214(c). CTA's two international section 214 authorizations are conditioned on it abiding by the commitments and undertakings contained in its 2007 LOA. *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Section 310(b)(4) Requests*, File No. ITC-T/C-20070725-00285, Public Notice, 22 FCC Rcd 15266, 15268 (IB 2007) (*2007 Pro Forma Grant Public Notice*) ("[W]e condition grant of this pro forma transfer of control on China Telecom (USA) Corporation abiding by the commitments and undertakings contained in its July 17, 2007 [LOA] . . . .").

[4] Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate [CTA's] International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, at 1-2 (filed Apr. 9, 2020) (Executive Branch Recommendation to
(continued….)

supports our decisions to revoke the domestic authority and revoke and terminate the international authorizations issued to CTA, and the determination that further mitigation will not address the substantial national security and law enforcement risks.[5] Accordingly, we direct CTA 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 the Commission's adoption of the *Institution Order* on December 10, 2020 is discussed in detail therein.[6] As the Commission 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 . . . ."[7] 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.[8] The Commission has taken a number of targeted steps to protect the nation's communications infrastructure from potential security threats,[9] and we continue to do so here.

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

(Continued from previous page)
Revoke and Terminate) (filing with the Commission a public filing, a non-public business confidential filing, and a classified appendix); *see also Institution Order*, 35 FCC Rcd at 15011-12, para. 9.

[5] *See infra* Section III.E. The Commission took official notice of the Recommendation and the classified information submitted by the Executive Branch agencies with its Recommendation. *Institution Order*, 35 FCC Rcd at 15014, para. 15, n.48 (citing 47 U.S.C. § 154(j) and *Use of Classified Information; Policy to be Followed in Future Licensing of Facilities for Overseas Communications*, Order, FCC 78-755, 44 Rad. Reg. 2d 607, 611, para. 10 (1978) (*Use of Classified Information Order*)).

[6] *See Institution Order*, 35 FCC Rcd at 15011-14, paras. 9-14.

[7] 47 U.S.C. § 151; *Institution Order*, 35 FCC Rcd at 15007, para. 2 (quoting 47 U.S.C. § 151); *see Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423 (2019) (*Protecting Against National Security Threats Order*), *aff'd*., *Huawei Technologies USA, Inc. v. FCC*, 2 F.4th 421, 439 (5th Cir. 2021) (*Huawei Technologies USA, Inc. v. FCC*).

[8] 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 National Security Threats Order*, 34 FCC Rcd at 11436, para. 34, *aff'd*. *Huawei Technologies USA v. FCC*, 2 F.4th at 439.

[9] *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*, 35 FCC Rcd at 15007, para. 2.

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 . . . ."[10] 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.[11] 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.[12] The Commission similarly considers the public interest to determine whether revocation of an international section 214 authorization is warranted. For example, in the *Foreign Participation Order* and the *Reconsideration Order*, the Commission delineated a non-exhaustive list of circumstances where it reserved the right to designate for revocation an international section 214 authorization based on public interest considerations.[13] The Commission initiated revocation proceedings concerning section 214 authorizations in a variety of contexts.[14]

[10] 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*).

[11] *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.

[12] *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.

[13] *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).

[14] *See, e.g.*, *Institution Order*; *China Unicom (Americas) Operations Limited*, 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) (*China Unicom 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 (continued….)

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.[15] With regard to this factor, the Commission has sought the expertise of the relevant Executive Branch agencies for over 20 years, and has accorded deference to their expertise in identifying such a concern.[16] 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).[17] 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.[18]

(Continued from previous page)
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) (*OneLink Order to Show Cause*).

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

[16] *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.

[17] *See generally Executive Branch Process Reform Report and Order*; 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, 19643 (Apr. 8, 2020) (Executive Order 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)).

[18] *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.").

6. *CTA's Section 214 Authority*. CTA holds two international section 214 authorizations, ITC-214-20010613-00346 and ITC-214-20020716-00371,[19] which are conditioned on CTA abiding by the commitments and undertakings contained in its 2007 LOA to the Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), and the Department of Homeland Security (DHS).[20] CTA is also authorized to provide domestic interstate telecommunications service[21] pursuant to blanket section 214 authority that the Commission has issued by rule.[22]

[19] A detailed procedural history of CTA's authorizations can be found in the *Order to Show Cause*. *Order to Show Cause*, 35 FCC Rcd at 3714-15, paras. 2-4; *id.* at paras. 3-4 ("On July 20, 2001, the International Bureau granted China Telecommunications Corporation an international section 214 authorization, ITC-214-20010613-00346, to provide global or limited global facilities-based and resale service between the United States and all permissible points, except China. On September 12, 2002, the International Bureau issued a Public Notice of a *pro forma* assignment of the international section 214 authorization, ITC-214-20010613-00346, from China Telecommunications Corporation to China Telecom (USA) Corporation, which was consummated on June 7, 2002. On August 21, 2002, the International Bureau granted China Telecom (USA) Corporation an international section 214 authorization, ITC-214-20020716-00371, to provide global or limited global facilities-based and resale service between the United States and China, subject to dominant carrier regulation on the U.S.-China route. On July 25, 2007, China Telecom (USA) Corporation notified the Commission of a *pro forma* transfer of control of the international section 214 authorizations, ITC-214-20020716-00371 and ITC-214-20010613-00346, held by China Telecom (USA) Corporation, from China Telecommunications Corporation to China Telecom Corporation Limited . . . consummated on July 12, 2007. On August 9, 2007, the [DHS], with the concurrence of the [DOJ] and the [FBI], filed a Petition to Adopt Conditions to Authorizations and Licenses. . . . On August 15, 2007, the International Bureau conditioned grant of the pro forma transfer of control on China Telecom (USA) Corporation abiding by the terms of the commitments and undertakings. According to Commission records, China Telecom (USA) Corporation notified the Commission by letter dated July 20, 2007 of a name change to [CTA]."); *see International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18); Cable Landing License Applications (47 C.F.R. § 1.767)*; *Requests to Authorize Switched Services over Private Lines (47 C.F.R. § 63.16)*; *Section 310(b)(4) Requests*, File No. ITC-214-20010613-00346, Public Notice, 16 FCC Rcd 14695, 14696 (2001) (*2001 Public Notice*); *International Authorizations Granted*; *Section 214 Applications (47 C.F.R. § 63.18)*; *Cable Landing License Applications (47 C.F.R. § 1.767)*; *Requests to Authorize Switched Services over Private Lines (47 C.F.R. § 63.16); Section 310(b)(4) Requests*, File No. ITC-214-20020716-00371, Public Notice, 17 FCC Rcd 16199, 16201 (2002) (*2002 Public Notice*).

[20] *2007 Pro Forma Grant Public Notice*, 22 FCC Rcd at 15268. The 2007 LOA requires CTA to (1) "make . . . U.S. Records available in the United States in response to lawful U.S. process"; (2) "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]"; (3) "not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, domestic communications or to any information (including the content of communications) pertaining to a wiretap order, pen/trap order, subpoena, or other lawful demand by a U.S. law enforcement agency for U.S. Records, to any person if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of the FBI, DOJ and DHS or the authorization of a court of competent jurisdiction in the United States"; (4) "maintain one or more points of contact within the United States with the authority and responsibility for accepting and overseeing compliance with a wiretap order, pen/trap order, subpoena or other lawful demand by U.S. law enforcement authorities for the content of communications or U.S. Records"; and (5) "notify the FBI, DOJ and DHS if there are material changes in any of the facts as represented in [the 2007 LOA] or if [CTA] undertakes any actions that require notice to or application to the FCC." 2007 LOA at 2-3. The 2007 LOA defines U.S. Records as "all customer billing records, subscriber information, and any other related information used, processed, or maintained in the ordinary course of business relating to communications services offered to U.S. persons." *Id.* at 2.

[21] CTA June 8, 2020, Response, Exh. 6 at 1-2; China Telecom (USA) Corporation, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20070725-00285, Attach. 1 at 2 (filed July 25, 2007); 2007 LOA at 1.

[22] 47 CFR § 63.01; *see supra* para. 4 & note 12.

7. CTA is a Delaware corporation that is indirectly and ultimately owned and controlled by the government of the People's Republic of China.[23] CTA is a direct, wholly owned subsidiary of China Telecom Corporation Limited (CTCL), an entity that is listed on the Hong Kong Stock Exchange as of CTA's June 8, 2020 Response.[24] CTCL is incorporated in the People's Republic of China.[25] China Telecommunications Corporation (CT), a corporation organized under Chinese law, holds, as of April 30, 2020, approximately 70.89% of the outstanding shares of CTCL.[26] The remaining outstanding shares are

[23] CTA June 8, 2020, Response, Exh. 1 at 1-2; *id.*, Exh. 1-1; *Order to Show Cause*, 35 FCC Rcd at 3715, para. 6. CTA was formerly known as China Telecom (USA) Corporation. *Order to Show Cause*, 35 FCC Rcd at 3713, para. 1, n.1; *see* China Telecom (Americas) Corporation, FCC Foreign Carrier Affiliations Notification, File No. FCN-NEW-20140917-00014, Attach. 1 at 1, n.1 (filed Sept. 17, 2014).

[24] CTA June 8, 2020, Response, Exh. 1 at 1 (noting that the shares of CTCL are publicly traded on the New York Stock Exchange (NYSE) and the Stock Exchange of Hong Kong Limited); *Order to Show Cause*, 35 FCC Rcd at 3716, para. 6; *but 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 11 (filed Jan. 14, 2021) (stating that an executive order was issued on November 12, 2020 "prohibiting transactions in publicly traded securities after finding a threat was posed by securities investments that finance Communist Chinese military companies and identifying one of [CTA's] parent entities as such a company") (citing *id.*, Exh. 130 at EB-3011, Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies, Exec. Order 13959, 85 Fed. Reg. 73185 (Nov. 12, 2020), https://www federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies) (Executive Branch Response)); *id.*, Exh. 130 at EB-3011-15. On January 6, 2021, NYSE announced the NYSE Regulation's decision to delist CTCL, China Mobile Limited, and China Unicom (Hong Kong) 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* China Telecom Corporation Limited, *Overview*, https://www.chinatelecom-h.com/en/company/company_overview.php (last visited Oct. 4, 2021); China Telecom Corporation Limited, Report of Foreign Private Issuer (Form 6-K), Exh. 1.1 at A-1, Completion of A Share Offering and Amendments to the Articles of Association (Aug. 18, 2021), https://www.sec.gov/Archives/edgar/data/0001191255/000119312521250231/d221686d6k.htm (stating, "A Shares of the Company will be listed and commence trading on the Shanghai Stock Exchange on 20 August 2021.") (CTCL Aug. 18, 2021 Form 6-K).

[25] CTA June 8, 2020 Response, Exh. 1 at 1; *Order to Show Cause*, 35 FCC Rcd at 3716, para. 6.

[26] CTA June 8, 2020 Response, Exh. 1 at 1; *id.*, Exh. 1-1; *Order to Show Cause*, 35 FCC Rcd at 3716, para. 6. *See also* China Telecom Corporation Limited, *Shareholding Structure* (updated Sept. 24, 2021), https://www.chinatelecom-h.com/en/company/structure.php; China Telecom Corporation Limited, Report of Foreign Private Issuer (Form 6-K), Exh. 1.1 at A-1, Determination of the Offer Size and Offer Price for the A Share Offering (Aug. 6, 2021), https://www.sec.gov/Archives/edgar/data/0001191255/000119312521238324/d186550d6k htm; China Telecom Corporation Limited, Report of Foreign Private Issuer (Form 6-K), Exh. 1.1 at A-19, Announcement of Interim Results for the Six Months Ended 30 June 2021 (Aug. 10, 2021), https://www.sec.gov/Archives/edgar/data/0001191255/000119312521241096/d169023d6k htm; CTCL Aug. 18, 2021 Form 6-K, Exh. 1.1 at A-1 and A-2; China Telecom Corporation Limited, Report of Foreign Private Issuer (Form 6-K) (CTCL Aug. 20, 2021 Form 6-K), Exh. 1.1 at 8, Articles of Association of China Telecom Corporation Limited, Article 22 (Aug. 20, 2021), https://www.sec.gov/Archives/edgar/data/1191255/000119312521252463/d167235d6k htm (Articles of Association of CTCL as of Aug. 20, 2021); China Telecom Corporation Limited,

(continued….)

held, as of CTA's June 8, 2020 Response to the *Order to Show Cause*, by: (1) entities registered or organized under the laws of the People's Republic of China (11.96%)[27] and (2) shareholders trading on the public exchange (17.15%).[28] CT is 100% directly owned by the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization.[29]

8. According to CTA, it "provides communications and Internet-based services to its customers by leasing lines from other carriers and providing the switching, routing and related equipment and value-added services necessary to meet customer request for services."[30] CTA states that some of its "telecommunications capabilities are provided as common carrier services pursuant to domestic and/or international section 214 authorizations, while some are provided on a private carrier basis."[31] CTA states that it offers the following services that it describes as "Communications and Internet Services" and that appear to be offered pursuant to CTA's section 214 authority: Mobile Virtual Network Operator (MVNO) service, International Private Leased Circuit (IPLC) service, International Ethernet Private Line (IEPL) service, and Multiple Protocol Label Switching/Virtual Private Network (MLPS VPN) service.[32] CTA is authorized to provide any other domestic telecommunications service under blanket section 214 authority,[33] and to provide "international basic switched, private line, data, television and business

(Continued from previous page)
Report of Foreign Private Issuer (Form 6-K), Exh. 1.1 at A-1, Announcement on the Plan to Increase Shareholding by the Controlling Shareholder (Sept. 21, 2021), https://www.sec.gov/Archives/edgar/data/0001191255/000119312521277986/d207552d6k htm; China Telecom Corporation Limited, Report of Foreign Private Issuer (Form 6-K), Exh. 1.1 at A-1 to A-4, Announcement on the Implementation of the Over-Allotment Option for the Initial Public Offering of A Shares (Sept. 24, 2021), https://www.sec.gov/Archives/edgar/data/0001191255/000119312521281541/d117447d6k htm. We note, based on publicly available information, that following the listing of the A shares of CTCL on the Shanghai Stock Exchange, CTCL remains majority-owned by CT.

[27] CTA states in its June 8, 2020 Response that the entities registered or organized under the laws of the People's Republic of China are Guangdong Rising Assets Management Co. Ltd. (6.94%); Zhejiang Financial Development Company (2.64%); Fujian Investment & Development Group co., Ltd. (1.2%); and Jiangsu Guoxin Group Limited (1.18%). CTA June 8, 2020 Response, Exh. 1 at 1. *See supra* note 26.

[28] CTA June 8, 2020 Response, Exh. 1 at 1. In its June 8, 2020 Response to the *Order to Show Cause*, CTA states that "17.15% of CTCL shares are widely held by shareholders trading on the public exchange," and identifies several shareholder entities. *Id.* In light of the delisting of CTCL from NYSE, we note that CTA's June 8, 2020 Response may not reflect the most recent information.

[29] *Id.*, Exh. 1-1; *id.*, Exh. 1 at 1 ("CT is a corporation incorporated in Beijing, China, with its capital invested by the State-owned Assets Supervision and Administration Commission of the State Council ('SASAC') of the People's Republic of China."); *Order to Show Cause*, 35 FCC Rcd at 3715-16, para. 6.

[30] CTA June 8, 2020 Response, Exh. 6 at 1. CTA states that it provides the following "Communications and Internet Services": International Private Leased Circuits; International Ethernet Private Lines; Global Wavelength; Ethernet over MPLS; Multiple Protocol Label Switching/Virtual Private Network (MPLS-VPN); Internet Protocol Security VPN; Global Internet Service using both ChinaNet (AS 4134) and CN2 (AS 4809); Mobile Virtual Network Operator (MVNO) services; and SIP Trunking. *Id.*, Exh. 6 at 2-6. CTA further states that it provides the following other services, which it identifies as "Other Non-Communications Services" and argues are not telecommunications services: Internet Data Center Services; Cloud Service; Virtual Private Cloud; SD-WAN; customer premises equipment; equipment leasing; Project Item service; NetCare ("an optional managed service . . . to deliver real-time, proactive connectivity monitoring and network troubleshooting to clients"); Maintenance Service; and Anti-DDoS service. *Id.*, Exh. 6 at 6-8. CTA also states that it provides Cloud Exchange, Global Media Distribution & Exchange, and professional Information and Communications Technologies service, which it identifies as "Other Non-Communications Services." *Id.*, Exh. 6 at 6-9.

[31] *Id.*, Exh. 6 at 1.

[32] *Id.*, Exh. 6 at 1-6.

[33] 47 CFR § 63.01; 47 U.S.C. § 214

services" under section 214 of the Act and its implementing rules.[34] This authority allows a carrier to continue to extend its existing network, install new equipment or upgrade existing equipment on its network, or request additional interconnections with the networks of other U.S. common carriers[35]—all without seeking further Commission approvals.[36]

9. *Executive Branch Recommendation to Revoke and Terminate.* On April 9, 2020, the National Telecommunications and Information Administration (NTIA) of the Department of Commerce filed a recommendation on behalf of the Executive Branch agencies requesting that the Commission revoke and terminate CTA's international section 214 authorizations.[37] In the filing, the Executive Branch agencies state that "[t]his recommendation reflects the substantial and unacceptable national security and law enforcement risks associated with [CTA's] continued access to U.S. telecommunications infrastructure pursuant to its international Section 214 authorizations."[38] The Executive Branch agencies submitted a separate classified appendix with additional information relevant to the recommendation and state that "the unclassified information alone is sufficient to support [their] recommendation."[39]

[34] 47 CFR §§ 63.22(d), 63.23(c), 63.18(e)(1)-(2); 47 U.S.C. § 214; *see supra* note 19.

[35] 47 U.S.C. § 214; 47 CFR § 63.02(a); *see also China Mobile USA Order*, 34 FCC Rcd at 3377, para. 33, n.98 (stating that China Mobile International (USA) Inc. (China Mobile USA) would be able to request interconnection with the networks of other U.S. common carriers).

[36] *See infra* para. 66 & note 301; CTA June 8, 2020 Response, Exh. 16 at 20 ("CTA is ineligible to hold a common carrier radio license under Section 310(b)(3) of the Communications Act, 47 U.S.C. § 310(b)(3), because all of its stock is owned by CTCL'[sic], a corporation organized under foreign law, so it cannot offer facilities-based mobile services."); *see also* Executive Branch Recommendation to Revoke and Terminate at 11-12 (stating, "[w]ith its current authorizations, [CTA] can . . . provide facilities-based mobile wireless services using its own network facilities instead of reselling mobile services as it currently does as an MVNO—all without seeking further FCC approvals under Section 214").

[37] Executive Branch Recommendation to Revoke and Terminate. The Executive Branch agencies that jointly made this recommendation are DOJ, DHS, DOD, the Departments of State and Commerce, and USTR. *Id*. at 1, n.1. These agencies are collectively referred to as the Executive Branch agencies. The Executive Branch agencies are either Members of or Advisors to the Committee created pursuant to Executive Order 13913. Executive Order 13913, 85 Fed. Reg. at 19643-44. DOJ, DHS, and DOD also are known informally as "Team Telecom."

[38] Executive Branch Recommendation to Revoke and Terminate at 1; *see also Institution Order*, 35 FCC Rcd at 15011-12, para. 9 (identifying the arguments that the Executive Branch agencies presented as grounds for their recommendation).

[39] Executive Branch Recommendation to Revoke and Terminate at 2; *see infra* Section III.E.; *see also Institution Order*, 35 FCC Rcd at 15012, paras. 9-10 & n.36. On December 8, 2020, DOJ filed with the Commission a notice "that the United States has recently initiated a proceeding against [CTA] in federal district court to determine whether the surveillance at issue was lawfully authorized and conducted." Letter from John C. Demers, United States Assistant Attorney General, National Security Division, U.S. Department of Justice, Loyaan A. Egal, Deputy Chief for Telecommunications, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, Alice Suh Jou, Attorney, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, to Marlene H. Dortch, Secretary, FCC at 1 (Dec. 8, 2020) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285); *Institution Order*, 35 FCC Rcd at 15012, para. 10, n.36; *see United States v. China Telecom (Americas) Corp.*, No. 20-mc-116, ECF No. 1 (D.D.C. filed Nov. 24, 2020). On November 24, 2020, the United States filed with the U.S. District Court for the District of Columbia a petition to initiate a determination that the Foreign Intelligence Surveillance Act (FISA) surveillance at issue was lawfully authorized and conducted. United States' Petition to Initiate a Determination that Certain FISA Surveillance was Lawfully Authorized and Conducted, *United States v. China Telecom (Americas) Corp.*, No. 20-mc-116, ECF No. 1 (D.D.C. filed Nov. 24, 2020). On September 2, 2021, the district court granted the government's petition. *Id.* ECF Nos. 16 & 18 (D.D.C. Sept. 2, 2021; redacted version released Sept. 16, 2021), *appeal pending*, No. 21-5215 (D.C. Cir. filed Sept. 30, 2021). CTA filed a notice of appeal to the United States Court of Appeals for the District of Columbia Circuit on September 30, 2021. *Id.* ECF No. 19.

10. *Order to Show Cause*. On April 24, 2020, the International Bureau, Wireline Competition Bureau, and Enforcement Bureau (the Bureaus) issued the *Order to Show Cause* directing CTA to file a response within thirty (30) calendar days demonstrating why the Commission should not initiate a proceeding to revoke and terminate CTA's domestic and international section 214 authorizations.[40] Among other things, the Bureaus noted the views of the Executive Branch agencies that there are "'substantial and unacceptable national security and law enforcement risks associated with [CTA's] continued access to U.S. telecommunications infrastructure pursuant to its international Section 214 authorizations.'"[41] The *Order to Show Cause* also directed CTA to respond to certain questions concerning its ownership, operations, and other related matters; to provide "a description of the extent to which [CTA] is or is not otherwise subject to the exploitation, influence, and control of the Chinese government"; and to provide "a detailed response to the allegations raised in the [Executive Branch Recommendation to Revoke and Terminate]."[42] On June 8, 2020, CTA filed its response to the *Order to Show Cause*, including a public filing and a non-public business confidential filing.[43]

11. *Institution Order*. In December 2020, the Commission issued the *Institution Order*, which instituted proceedings to revoke the domestic authority and revoke and/or terminate the international authorizations issued to CTA pursuant to section 214 of the Act.[44] The Commission stated that it "find[s] that [CTA] has failed to rebut the serious concerns of the Executive Branch about its continued presence in the United States and thus adopt[s] procedures that will allow for [CTA], Executive Branch agencies, and the public to present any remaining arguments or evidence in this matter."[45] The Commission explained that "[t]his proceeding affords [CTA] additional notice and an opportunity to file a written submission to explain whether the public interest, convenience, and necessity are served by its retention of its domestic and international section 214 authorizations, and why the Commission should not revoke and/or terminate its domestic and international section 214 authority."[46] The Commission also denied the Application for Review filed by CTA[47] and directed the International Bureau to provide to DOJ, in its capacity as chair of the Committee, information submitted in confidence by CTA.[48]

---

[40] *See generally Order to Show Cause*; *see also id.*, 35 FCC Rcd at 3713, 3718, 3720, paras. 1, 12, 14. Additional discussion of the procedural history related to the *Order to Show Cause* can be located in the *Institution Order*. *See Institution Order*, 35 FCC Rcd at 15012-13, para. 11 & nn.37-40.

[41] *Order to Show Cause*, 35 FCC Rcd at 3713, para. 1 (quoting Executive Branch Recommendation to Revoke and Terminate at 1).

[42] *Id.*, 35 FCC Rcd at 3718-19, para. 12.

[43] CTA June 8, 2020, Response; *see also Institution Order*, 35 FCC Rcd at 15013, para. 11 & n.40.

[44] *See generally Institution Order*; 47 U.S.C. § 214.

[45] *Institution Order*, 35 FCC Rcd at 15006-07, para. 1.

[46] *Id.* at 15015, para. 16.

[47] *Id.* at 15007, para. 1; *see also id.* at 15014-15, 15042-45, paras. 15, 62-70. On July 8, 2020, DOJ filed, on behalf of the Attorney General as the Chair of the Committee, a letter requesting disclosure of certain information in this matter for which CTA had requested confidential treatment. *Id.* at 15013, para. 12. CTA objected to the disclosure. *Id.* On August 17, 2020, the International Bureau informed CTA that pursuant to section 0.442 of the Commission's regulations, the International Bureau intended to disclose to DOJ, and through DOJ, to the Members of and Advisors to the Committee, certain information submitted to the Commission in confidence by CTA, subject to the provisions of 44 U.S.C. § 3510(b). *Id.* at 15014, para. 13. On August 31, 2020, CTA filed an Application for Review. *Id.* at 14. A detailed discussion of the procedural history can be located in the *Institution Order*. *See id.* at 15013-14, paras. 12-14.

[48] *Id.* at 15007, 15014-15, paras. 1, 15. Following the issuance of the *Institution Order*, CTA filed with the Commission a motion for stay. China Telecom (Americas) Corporation, Motion to Stay Disclosure of China Telecom (Americas) Corporation's Confidential Information, GN Docket No. 20-109, at 11 (filed Dec. 21, 2020). On December 23, 2020, CTA filed with the United States Court of Appeals for the Fourth Circuit (Fourth Circuit) a (continued….)

12. On December 23, 2020, CTA filed with the Fourth Circuit a petition for review of the *Institution Order*.[49] On January 22, 2021, CTA filed a motion for expedited briefing and consideration of its petition for review.[50] On May 10, 2021, the Fourth Circuit granted the Commission's motion and dismissed CTA's petition for lack of jurisdiction, stating that the Order which CTA sought to appeal "is neither a final agency action nor an appealable interlocutory or collateral order."[51]

13. *Comments*. Any comments filed by the public, including the Committee, responding to CTA's June 8, 2020 Response to the *Order to Show Cause* were due by January 19, 2021.[52] Any filing by CTA demonstrating why the Commission should not revoke and/or terminate its section 214 authority was due no later than March 1, 2021.[53] On January 14, 2021, the Executive Branch agencies filed comments responding to CTA's June 8, 2020 Response.[54] In addition, more than 150 individual comments were filed by the public.[55] On March 1, 2021, CTA filed reply comments responding to the *Institution Order* and the Executive Branch Response.[56]

(Continued from previous page)
motion for stay. Petitioner China Telecom (Americas)'s Motion to Stay Pending Judicial Review at 1, *China Telecom (Americas) Corp. v. FCC*, No. 20-2365 (4th Cir. filed Dec. 23, 2020). The Fourth Circuit denied CTA's motion for stay on January 13, 2021. *China Telecom (Americas) Corp. v. FCC*, No. 20-2365 (4th Cir. Jan. 13, 2021). Following the Fourth Circuit's denial of CTA's motion for stay, Commission staff provided to DOJ and the Committee the requested unredacted confidential exhibits of CTA's response to the *Order to Show Cause*, as requested by DOJ on behalf of the Attorney General as the Chair of the Committee.

[49] Petition for Review, *China Telecom (Americas) Corp. v. FCC*, No. 20-2365 (4th Cir. filed Dec. 23, 2020).

[50] Petitioner China Telecom (Americas)'s Motion for Expedited Briefing and Consideration, *China Telecom (Americas) Corp. v. FCC*, No. 20-2365 (4th Cir. filed Jan. 22, 2021). On January 22, 2021, the Fourth Circuit directed the Commission to respond to CTA's motion to expedite on or before February 1, 2021. *China Telecom (Americas) Corp. v. FCC*, No. 20-2365, at 1 (4th Cir. Jan. 22, 2021). On February 1, 2021, the Commission filed an opposition to CTA's motion to expedite and a motion to dismiss CTA's petition for review. Respondents' Opposition to Motion to Expedite, *China Telecom (Americas) Corp. v. FCC*, No. 20-2365 (4th Cir. filed Feb. 1, 2021); Respondents' Motion to Dismiss, *China Telecom (Americas) Corp. v. FCC*, No. 20-2365 (4th Cir. filed Feb. 1, 2021). Following the submission of additional filings, the Fourth Circuit directed an accelerated briefing schedule on February 16, 2021. *China Telecom (Americas) Corp. v. FCC*, No. 20-2365, at 1 (4th Cir. Feb. 16, 2021) (directing the filing of the opening brief and joint appendix by March 2, 2021, the response brief by April 1, 2021, and the reply brief by April 15, 2021).

[51] *China Telecom (Americas) Corp. v. FCC*, No. 20-2365, at 1 (4th Cir. May 10, 2021). In light of the Fourth Circuit's decision granting the Commission's motion and dismissing CTA's petition, we determine that CTA's request to hold our decision in abeyance is moot. *See* CTA March 1, 2021 Reply at 3 ("Because the Fourth Circuit Court of Appeals has adopted an expedited briefing schedule for its consideration of CTA's petition for review of the Order Instituting Proceedings, the Commission should not conduct any further adjudication in this proceeding until the court has reached a decision in that matter.").

[52] *Institution Order*, 35 FCC Rcd at 15045, 15046, paras. 71, 76.

[53] *Id*.

[54] *See* Executive Branch Response. For purposes of this filing, the Executive Branch Response includes the interested agencies listed in the April 9, 2020 Executive Branch Recommendation to Revoke and Terminate. *Id*. at 1, n.2; Executive Branch Recommendation to Revoke and Terminate at 1, n.1. On January 19, 2021, the Executive Branch agencies filed an errata and a corrected Index of Exhibits. Executive Branch Response, Errata (filed Jan. 19, 2021) (filing a corrected Index of Exhibits to correct page numbers for the Executive Branch Response).

[55] We observe that some commenters filed identical comments more than once.

[56] *See* CTA Mar. 1, 2021 Reply at 1. On October 8, 2021, CTA filed an *ex parte* letter. Letter from Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, GN Docket No. 20-109 (filed Oct. 8, 2021) (CTA *Ex Parte* Letter).

III. DISCUSSION

14. After providing CTA 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 extensive unclassified record alone, that the present and future public interest, convenience, and necessity is no longer served by CTA'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. We then discuss the overwhelming record evidence mandating that we revoke CTA's domestic section 214 authority and revoke and terminate CTA's international section 214 authorizations, including how the classified evidence submitted by the Executive Branch agencies further supports our decisions here and our finding that further mitigation will not address the substantial and unacceptable national security and law enforcement concerns.

A. Standard of Review

1. Applicable Standard of Proof

15. 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 CTA's domestic section 214 authority and revocation and termination of its international section 214 authorizations is warranted.[57] Contrary to CTA's assertion to apply a clear and convincing standard of proof, and as stated in the *Institution Order*, 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."[58] The Executive Branch agencies support this view, stating that "CTA incorrectly imports the burden of proof found in [section 312(d) and section 1.91(d)] [which] do not apply to Section 214 authorizations . . . [because] by their terms, they apply to revocations of *radio* licenses."[59] The Executive Branch agencies also argue that CTA cites an obsolete case to support its argument that the clear and convincing standard of proof applies here.[60] Additionally, no commenter specifically disputed the Commission's preliminary view.[61] We agree with the Executive Branch agencies and reject CTA's argument that the clear and convincing standard should apply in this case. We therefore find, consistent with applicable law, that the appropriate standard of proof in this proceeding is the preponderance of the evidence standard.

---

[57] *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).

[58] *Institution Order*, 35 FCC Rcd at 15014, para. 15, n.49 (citing *Steadman*, 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)); *see* CTA June 8, 2020 Response, Exh. 16 at 8 ("[R]evocation of an FCC license is governed, at the agency level, by the 'clear and convincing' standard of proof …." (citing *Sea Island*, 627 F.2d at 244)).

[59] Executive Branch Response at 4 (citing CTA June 8, 2020 Response, Exh. 16 at 8, n.10).

[60] *Id*. at 5. CTA relies 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. *Sea Island*, 627 F.2d at 244. *See* CTA June 8, 2020 Response, Exh. 16 at 8. CTA ignores the fact that 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*. 450 U.S. at 104.

[61] As a related matter, CTA argues that "[b]y inviting parties to comment on the appropriate standard of proof, the Commission tacitly admits the existence of material disputed facts that warrant an evidentiary hearing." CTA Mar. 1, 2021 Reply at 30. We address this argument below. *See infra* para. 40.

2. Public Interest Standard

16. We also reject CTA's arguments that "revocation must be justified by some act of the regulated party, not based on speculation or attenuated and nebulous changes in circumstance or foreign policy considerations that are beyond a licensee's control."[62] In particular, CTA argues that section 312(a)(2) "implies that there must be some act or omission of the licensee that warrants revocation"[63] and that "Commission practice confirms this, as revocation invariably results from some particularized concern about the licensee's conduct, character, or other qualifications."[64] Moreover, CTA argues that "[s]ection 312(a)(2) does not permit revocation based on facts that were actually presented in the original application."[65] The Executive Branch agencies assert that "Commission precedent does not limit revocation to egregious misconduct,"[66] contending that "[CTA] inaccurately refers to non-binding policy statements and staff-level orders as Commission 'precedent.'"[67] The Executive Branch agencies argue that "[i]t is well-settled that there would be independent grounds to revoke a license based on a finding of an intentional misrepresentation to the Commission."[68] They further argue that "[r]evocation could be warranted, for example, by arguably 'subtle' or 'hyper-technical misrepresentations' about a radio station owner's involvement in a licensee's operations"[69] because "the FCC relies heavily on the honesty and probity of its licensees in a regulatory system that is largely self-policing; misrepresentations do not need to be egregious to impair effective regulation if an agency can no longer depend on the representations made by licensees."[70]

17. We affirm the Commission's prior determination that it is unreasonable to conclude that "some act of a regulated party," such as egregious misconduct, could be the only justification for revocation,[71] given the Commission's ongoing responsibility to evaluate all aspects of the public interest, including national security and law enforcement concerns that are "independent of our competition analysis."[72] 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

[62] CTA Mar. 1, 2021 Reply at 38. CTA argues that the Commission "has alleged misconduct in all cases where it has revoked a Section 214 license, in all cases where it issued a show cause or admonishment order, and in all cases where it considered initiating revocation proceedings." *Id*. at 39-40 (citing case law).

[63] *Id*. at 41.

[64] *Id*. (citing *KWK Radio, Inc. v. FCC*, 337 F.2d 540 (D.C. Cir. 1964); *Theodore E. Sousa*, 93 FCC 2d 1064 (Rev. Bd. 1983); *Roger Thomas Scaggs*, 19 FCC Rcd 7123 (EB 2004)).

[65] *Id*. at 41-42 (citing *Trans Video Communications, Inc.*, 22 FCC Rcd 855, 860-61, para. 16 (WTB 2007); *Theodore E. Sousa*, 92 FCC 2d 173 (1982)). CTA adds that "[t]hus, the Commission cannot revoke CTA's authorization solely because its corporate parent is ultimately controlled by a Chinese state-owned enterprise, as these facts were disclosed both in the original [s]ection 214 applications and in the *pro forma* transfer of control notification that led to the approval of the [Letter of Assurances]." *Id*. at 42.

[66] Executive Branch Response at 5.

[67] *Id*.

[68] *Id*. at 6 (citing *Contemporary Media Inc. v. FCC*, 214 F.3d 187, 196-98 (D.C. Cir. 2000)).

[69] *Id*.

[70] *Id*. (citing *Contemporary Media*, 214 F.3d at 193).

[71] CTA cites to Commission cases where revocation was based on a regulated entity's egregious misconduct. *See* CTA Mar. 1, 2021 Reply at 2, 15, n.49, 39.

[72] *Institution Order*, 35 FCC Rcd at 15016, para. 19 (citing *Foreign Participation Order*, 12 FCC Rcd at 23919, 23921, paras. 63, 65).

application."[73] As the Commission stated in the *Institution Order*, "[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'[74] and explained that it grants 'blanket' and 'global' authorizations with the understanding that they may be revoked."[75] We therefore find that 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.[76]

3. CTA Had Sufficient Notice and Several Opportunities to Be Heard

18. We reject CTA's various procedural arguments and find that the procedures the Commission followed are consistent with principles of due process and applicable law and provided CTA with sufficient notice and several opportunities to be heard.[77] In particular, CTA argues that a more formal hearing before an Administrative Law Judge is required by the Commission's rules to safeguard its due process rights.[78] CTA argues that the exceptions to the notice and opportunity requirements of section 558(c) of the Administrative Procedure Act (APA) do not apply here.[79] Finally, CTA asserts that the Commission cannot avoid a hearing by claiming that no material facts are in dispute.[80]

a. Procedures Are Consistent with the Commission's Rules, Past Practice, and Precedent

19. The procedures adopted in this matter are consistent with the Commission's rules, past practice, and precedent. Specifically, we reject CTA's contention that the Commission's decision not to designate this matter for a hearing was arbitrary and capricious because the Commission allegedly deviated from its own past practice and precedent without acknowledgement or justification.[81] CTA acknowledges that the Act is silent as to the substantive standards or processes for revocation of a section 214 authorization, but contends that the Commission through its consistent practice and precedent has determined that the same process that governs revocation of radio licenses under section 312(c) and (d) of

[73] 47 U.S.C. § 312(a)(2).

[74] *Institution Order*, 35 FCC Rcd at 15016, para. 19 (citing *Foreign Participation Order*, 12 FCC Rcd at 23900, para. 19).

[75] *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 ("[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.")).

[76] *Id.* at 15016, para. 19.

[77] CTA argues that the "opportunity" to respond to the allegations against it is largely illusory because CTA "has already responded once to the same allegations and the Commission has made clear that it will not accept CTA's position on any of the issues." CTA Mar. 1, 2021 Reply at 1-2. We disagree and note that despite its argument that the opportunity to submit additional arguments was illusory, CTA submitted a 63-page Reply.

[78] *Id*. at 4-23.

[79] *Id*. at 23-29.

[80] *Id*. at 29-37.

[81] *Id*. at 3-4, 9-10. CTA also argues that "[t]he FCC violated its own rules requiring a live hearing, which were intended to benefit parties like CTA by protecting due process rights and this violation prejudiced CTA. Likewise, the Commission failed to apply its own test to determine whether CTA's due process rights would be substantially protected, failing to even reference the [*Mathews v. Eldridge*] test in its Order Instituting Proceedings." *Id.* at 13.

the Act also governs revocation of section 214 authorizations.[82] CTA contends that "[t]his process includes notice, an opportunity to respond, and a hearing before an Administrative Law Judge to assess the reasons for revocation, including whether the evidence presented was sufficient to justify revocation."[83] CTA adds that the Commission has applied section 1.91 of the Commission's rules to revocation of section 214 authorizations, but acknowledges that this rule, by its terms, governs revocation and/or cease and desist orders concerning a radio station license or construction permit.[84]

20. As explained in the *Institution Order* and in similar cases,[85] 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"[86] 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."[87] 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,[88] it has used other procedures for different types of proceedings when 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.[89] 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.[90] In fact, in last year's *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."[91]

[82] *Id*. at 4.

[83] *Id*.

[84] *Id*. at 4-5; *see id.* at 5-9, 11.

[85] *Institution Order*, 35 FCC Rcd at 15015, para. 16; *China Unicom Americas Institution Order*, 36 FCC Rcd at 6328-29, para. 16; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6377-78, para. 14.

[86] 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").

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

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

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

[90] *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).

[91] *Administrative Hearings Order* at 10729, para. 2.

21. As we previously observed,[92] there is no statutory obligation that requires us to follow any specific procedures in the instant matter.[93] CTA identifies several cases between 1997 and 2007 in which the Commission designated for hearing the revocation of section 214 authorizations.[94] 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.[95] CTA acknowledges that "[t]he FCC has revoked Section 214 authorizations without referring issues to an Administrative Law Judge for an evidentiary hearing," but it asserts that this has occurred "only in cases where the respondent had gone out of business and did not respond to notice from the FCC."[96] Although CTA attempts to distinguish those proceedings,[97] they demonstrate that the Commission has not applied subpart B hearing rules[98] to all section 214 revocation proceedings.[99] Thus, contrary to CTA's view, the Commission has never had an

[92] *China Unicom Americas Institution Order*, 36 FCC Rcd at 6328-29, para. 16; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6377-78, para. 14.

[93] 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. 39-43.

[94] CTA Mar. 1, 2021 Reply at 5-7 (citing *CCN, Inc. Order to Show Cause*, 12 FCC Rcd 8547, *CCN, Inc. Order*, 13 FCC Rcd 13599; *Publix Network Corp.*, Order to Show Cause and Notice of Opportunity for Hearing, 17 FCC Rcd 11487 (2002), *Consent Order*, FCC 05M-12 (2005); *Business Options, Inc.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6881 (2003), *case terminated by consent*, 19 FCC Rcd 2916 (2004); *NOS Comm'cns, Inc., et al.*, Order to Show Cause and Notice of Opportunity for Hearing, 18 FCC Rcd 6952 (2003), *case terminated by consent*, FCC 03M-42 (2003); and *Kintzel Order*, 22 FCC Rcd 17197 (2007), *case terminated by consent*, FCC 09M-52 (2009)). Significantly, none of those matters were ultimately resolved through a hearing under the subpart B rules.

[95] *See China Unicom Americas Institution Order*, F36 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").

[96] CTA Mar. 1, 2021 Reply at 7. CTA also states that "[b]eginning in 2015 the FCC terminated, without evidentiary hearings, a series of authorizations held by carriers that allegedly breached their agreements with executive agencies. These companies had failed to respond to multiple contact attempts by the government and therefore were presumed to have gone out business." *Id*. at 7, n.21 (citing, for example, *Wypoint Telecom, Inc. Termination of International Section 214 Authorization*, Order, 30 FCC Rcd 13431, 13433, para. 4 (IB-PD 2015) (*Wypoint Telecom Order*); *LDC Telecommunications, Inc.*, File No. ITC-214-20080523-00238, Order to Pay or to Show Cause, 31 FCC Rcd 7228 (EB-TCD, IB-TAD & WCB-CPD 2016), Revocation Order, 31 FCC Rcd 11661, 11662, para. 5 (EB-TCD, IB-TAD & WCB-CPD 2016) (*LDC Telecommunications Order); WX Communications Ltd. Termination of International Section 214 Authorization*, Order, 34 FCC Rcd 1028, 1029-30, 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 others. *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*.

[97] CTA Mar. 1, 2021 Reply at 7.

[98] 47 CFR §§ 1.201-.377 (rules governing hearing proceedings).

[99] CTA also identified various cases where the Commission or the Bureaus, under delegated authority, ordered certain carriers to demonstrate why their domestic and/or international section 214 authority should not be revoked, but where the Commission or the Bureaus have not taken further action on such revocation. CTA Mar. 1, 2021 Reply at 8 (citing *Sandwich Isles Communications, Inc. et al.*, 31 FCC Rcd 12947, 12974, para. 84 (2016); *Sandwich Isles Communications, Inc. et al.*, 35 FCC Rcd 10831, 10855, para. 48 (2020); *OneLink Order to Show Cause*, 32 FCC Rcd at 1886, para. 8; *New Century Telecom, Inc.*, Admonishment Order, 31 FCC Rcd 5187 (EB-TCD 2016)).

established practice of requiring subpart B hearings for all section 214 revocations.[100] Rather, we find that the handful of cases on which CTA 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 CTA 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."[101] 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.[102] As we stated in the *China Unicom Americas Institution Order* and *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 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.[103]

22. More importantly, the Commission has never applied its subpart B hearing rules to every adjudication.[104] 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.[105] This distinction reflects one in the Act itself, which specifies a procedure for revoking

[100] *China Unicom Americas Institution Order*, 36 FCC Rcd at 6330, para. 18; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6379, para. 16. Nor would hearings be required in the termination of section 214 authority where, for example, the authorization holder failed to meet a condition of its international section 214 authorization such as meeting the terms of a mitigation agreement with the Executive Branch agencies.

[101] *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.

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

[103] *China Unicom Americas 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 CTA's argument that "[because] the FCC has repeatedly cited [Section 312(d) of the Act and Section 1.91 of the rules] in orders designating proposed revocation of Section 214 authorizations for hearing, [the FCC] has thereby adopted them as the relevant standards for Section 214 revocation proceedings." CTA Mar. 1, 2021 Reply at 5, n.9. *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).

[104] *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.* note 1.

[105] 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

(continued….)

Title III authorizations in section 312,[106] 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."[107]

b. Procedures Satisfy Due Process Requirements

23. We conclude that the procedures followed here satisfy the requirements of due process and that the Commission did not violate CTA's due process rights by denying its request for an evidentiary hearing. CTA argues that it is entitled to protections under the Due Process Clause because its section 214 authorizations are protected property interests[108] and that it will be "predictably deprived of its property interest without due process of law" if the Commission revokes its authorizations without an evidentiary hearing.[109] CTA asserts that "'[t]he [Supreme] Court has consistently held that some kind of hearing is required at some time before a person is finally deprived of his property interests'"[110] and that "due process usually requires a pre-deprivation hearing."[111] CTA contends that an evidentiary hearing is warranted because "[a]bsent a hearing, the tenor of the Order Instituting Proceedings makes it obvious that the outcome of the FCC's proceeding is preordained."[112] CTA adds that the Commission's rules already provide a process for administrative hearings and thus the Commission cannot assert that the "predeprivation process [is] impossible here."[113] Finally, CTA contends that the Commission arbitrarily and capriciously failed to consider the *Mathews v. Eldridge* three-part test, which the Commission stated in the *Administrative Hearings Order* is used by the presiding officer in a hearing context "[t]o determine whether due process requires live testimony in a particular case."[114]

(Continued from previous page)
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.").

[106] 47 U.S.C. § 312(c).

[107] *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 China Unicom Americas Institution Order*, 36 FCC Rcd at 6330, para. 17; *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6379, para. 15.

[108] CTA Mar. 1, 2021 Reply at 13 (citing *Spinelli v. New York*, No. 07-1237-cv, 2009 WL 2413929 (2d Cir. Aug. 7, 2009)). CTA argues that it has a protectable property interest because it has "'more than a unilateral expectation'" in its section 214 authorizations' continued effect. *Id*. at 13 (citing *3883 Conn. LLC v. Dist. of Columbia*, 336 F.3d 1068, 1072 (D.C. Cir. 2003).

[109] *Id*. at 16.

[110] *Id*. at 15 (citing *Wolff v. McDonnell*, 418 U.S. 539, 557–58 (1974); *see id.* at 15-16 ("The requirement for some kind of a hearing applies to the taking of private property, *Grannis v. Ordean*, 234 U.S. 385, 1363 (1914), the revocation of licenses, *In re Ruffalo*, 390 U.S. 544, 88 S.Ct. 1222, (1968), the operation of state dispute-settlement mechanisms, when one person seeks to take property from another, or to government-created jobs held, absent 'cause' for termination [citation omitted].")

[111] *Id*. at 16 (citing *Zinermon v. Burch*, 494 U.S. 113, 132 (1990) ("In situations where the State feasibly can provide a predeprivation hearing before taking property, it generally must do so.")).

[112] *Id*. at 16. Additionally, CTA asserts that "[t]he Commission's own rules provide a process for administrative hearings that, if followed, would protect CTA's due process rights against erroneous deprivation [and that] [i]t is the Commission's arbitrary and capricious decision to ignore those procedures that deprives CTA of due process of law." *Id*. at 17.

[113] *Id*. at 16 (citing *Zinermon*, 494 U.S. at 136-37).

[114] *Administrative Hearings Order,* 35 FCC Rcd at 10733, para. 12; *see* CTA Mar. 1, 2021 Reply at 17-23 (analyzing *Mathews v. Eldridge* factors in this case); *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976).

24. Contrary to CTA'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."[115] The procedural requirements for formal adjudications under the APA[116] do not apply here,[117] 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.'"[118] That is the case here; we conclude that the ultimate decisions about revocation and termination may be resolved on the present record. As the Commission previously noted, the proceedings here, including the Executive Branch Recommendation to Revoke and Terminate and the response to the *Order to Show Cause*, have already produced an "extensive" written record giving CTA the first opportunity to respond.[119] The *Institution Order* in turn provided CTA with a "further opportunity" to explain why "the public interest, convenience and necessity are served by its retention of its domestic and international section 214 authorizations."[120] Indeed, CTA submitted a 63-page Reply to the allegations against it.[121]

25. 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."[122] With regard to the first factor, CTA states that its business interests would be impaired if the loss of its section 214 authority forced it "to cease providing telecommunications services to U.S. customers on a common carrier basis."[123] While we recognize that revocation and termination will have an impact on CTA 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."[124]

---

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

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

[117] *See Administrative Hearings Order*, 35 FCC Rcd at 10732, para. 9 n.24 (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).

[118] *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).

[119] *Institution Order*, 35 FCC Rcd at 15015, para 17.

[120] *Id*. at 15014-15, paras. 16-17.

[121] CTA Mar. 1, 2021 Reply.

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

[123] CTA Mar. 1, 2021 Reply at 17-18. CTA further states that its local employees and customers could also be affected. *Id*.

[124] 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

(continued….)

26. With regard to the second *Mathews* factor, CTA has not shown the value of any additional process or how any additional process would prevent erroneous deprivation, and 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."[125] CTA has not persuasively explained why the process the Commission afforded it, in which CTA submitted two full rounds of written comments to respond to the specific bases for revocation and/or termination 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 CTA with timely and adequate notice of the reasons for revocation and/or termination; opportunity to respond with its own evidence and to make any factual, legal, or policy arguments; access to all of the unclassified evidence the Commission considers; and a written order from the Commission providing its preliminary reasoning for any adverse decision.

27. 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.[126] 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.[127] More importantly, given the national security issues at stake, any resulting unwarranted delay could be harmful.[128] As such, we are not persuaded by CTA's contention that "[f]or [it] to be meaningfully heard outweighs the burden that a live hearing would place on the FCC and actually advances the FCC's interest in accurately determining whether CTA's Section 214 authorization should be revoked."[129] CTA has given us no reason here to believe that live testimony would shed meaningful light on material facts.

28. Thus, our *Mathews* analysis supports our conclusion that no live testimony is required and that the process afforded to CTA here has been sufficient. Even if CTA 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.

29. Furthermore, the procedures in this case address CTA's "concerns about its ability to obtain a fair opportunity to rebut the factual assertions levied against it without a hearing by a neutral adjudicator such as an Administrative Law Judge."[130] Even under the subpart B hearing rules that CTA would have the Commission apply, a hearing may be presided over by "an administrative law judge,"

(Continued from previous page)
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.

[125] *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").

[126] *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).

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

[128] *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).

[129] CTA Mar. 1, 2021 Reply at 22-23 (citing *Kirk v. Comm'r of Soc. Sec. Admin*, No 1901989, 2021 WL 387022, at *10 (4th Cir. Feb. 4, 2021)).

[130] *Id*. at 22.

"one or more commissioners," or "the Commission" itself.[131] 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.[132] In any event, CTA 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 CTA been denied an opportunity to introduce evidence or arguments on its behalf, and the Commission's decision here is based on the entire record. With regard to the need for a "neutral" decisionmaker or adjudicator,[133] CTA argues that "[s]everal of the past and present Commissioners have spoken publicly about their desire to strip CTA of its ability to operate in the United States."[134] CTA fails, however, to argue with specificity why the Commission or any individual Commissioner would not be able to serve as a neutral decisionmaker in this case—and it has never moved for the recusal of any Commissioner.[135] 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.

30. Moreover, we are unpersuaded by CTA's contention that it cannot defend itself in this proceeding in accordance with its due process rights because it does not have access to undisclosed classified evidence.[136] In particular, CTA argues that it "has not received notice of *all* allegations against it and an opportunity to respond to them"[137] because "the Commission's decision to initiate revocation proceedings . . . was largely based on undisclosed information."[138] Therefore, CTA contends that its "ability to meaningfully probe or cross-examine that evidence is limited severely, thereby creating an unacceptably high risk of erroneous deprivation" and that a "live hearing provides one of the most important procedural safeguards to combat that risk."[139] We reject these arguments for the following reasons.

[131] 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).

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

[133] *See, e.g.*, CTA Mar. 1, 2021 Reply at 18, 21, 45, n.163.

[134] *Id*. at 22.

[135] CTA has not provided persuasive evidence to support its claim. Rather, it cites to an article where former Chairman Pai voiced concerns regarding Chinese espionage and threats to U.S. telecommunications networks, among other things. *Id*. (stating, "[s]everal of the past and present Commissioners have spoken publicly about their desire to strip CTA of its ability to operate in the United States," citing David Shepardson, Departing U.S. FCC chair warns of threats to telecoms from China, REUTERS (Jan. 20, 2021)). We note that former Chairman Pai's statement in the *Institution Order* expressed a similar concern. *Institution Order*, 35 FCC Rcd at 13048, Statement of Chairman Ajit Pai ("Taken together, these allegations raise serious doubts about whether [CTA] should be allowed to continue operating in the United States. And to date, the company has not provided the FCC with a satisfactory response to the concerns raised by the Executive Branch agencies. . . ."). The opinion of former Chairman Pai was based on the evidence at that time and the record evidence developed since then has not addressed those concerns.

[136] CTA Mar. 1, 2021 Reply at 19-20.

[137] *Id*. at 20 (citing 5 U.S.C. § 558(c))

[138] *Id*.

[139] *Id*.

31. *First*, the Commission lacks jurisdiction to consider CTA's challenge to our consideration of certain classified evidence. Section 1806 of the Foreign Intelligence Surveillance Act[140] vests exclusive jurisdiction in the district court for any request to "discover, obtain, or suppress" FISA material. CTA's position that the government either must provide it with a copy of the classified evidence or else may not consider it is in effect seeking either to discover or suppress FISA material, a matter over which Congress vested exclusive jurisdiction in the district court, and therefore the Commission lacks jurisdiction to accept CTA's arguments on this issue.[141]

32. *Second*, we independently find that due process permits the Commission to consider the classified material. Our reliance on classified information is permissible[142] as it is well established—and CTA agrees—that under appropriate circumstances—such as the availability of *in camera, ex parte* review by a federal district court under 50 U.S.C. § 1806(f)—the Due Process Clause permits an agency to "rel[y] on classified information" in administrative proceedings involving national security while requiring the government "only to disclose the unclassified portions of the record."[143] In any event, we find that our decision to revoke the domestic section 214 authority and revoke and terminate the international section 214 authorizations issued to CTA, and the determination that further mitigation will not address the substantial national security and law enforcement risks, would be warranted based solely on the unclassified information in the record without relying on any of the classified material.

c. Applicability of Section 558(c) of the Administrative Procedure Act

33. We find that the procedures the Commission adopted in this proceeding conformed with section 558(c) of the Administrative Procedure Act (APA)[144] by providing CTA with notice, in writing, of the issues in this proceeding, and giving CTA ample opportunities to "demonstrate or achieve compliance with all lawful requirements."[145] We agree with the Executive Branch agencies that CTA "has already

[140] 50 U.S.C. § 1806

[141] Furthermore, consideration of this argument may be foreclosed by collateral estoppel. In *United States v. China Telecom (Americas) Corp.*, the district court found that the "United States's FISA surveillance was lawfully authorized and conducted and that [CTA's] statutory and due process rights were not violated by an *in camera, ex parte* review as provided by statute." *United States v. China Telecom (Americas) Corp*., No. 20-mc-116, ECF Nos. 16 & 18, at 11 (D.D.C. Sept. 2, 2021), *appeal pending*, No. 21-5215 (D.C. Cir. filed Sept. 30, 2021). In reaching its decision, the district court squarely rejected CTA's arguments that it "has a protected property interest in its FCC license and that due process requires a hearing and an opportunity to respond to evidence against it," the identical arguments CTA raises in this proceeding. *Id.* at 6-7. Under the doctrine of collateral estoppel, because those "issue[s] [have been] actually and necessarily determined by a court of competent jurisdiction, that determination is conclusive in subsequent suits." *Montana v. United States*, 440 U.S. 147, 153 (1979). If affirmed by the D.C. Circuit on appeal, the district court's prior adjudication of CTA's arguments with respect to this classified evidence will be binding because (1) the identical issues were previously litigated; (2) the issues were actually litigated; (3) the previous determination was necessary to the decision; and (4) the party being precluded from relitigating the issues was fully represented in the prior action. *See, e.g.*, *United Industrial Workers v. Government of the Virgin Islands*, 987 F.2d 162, 169 (3d Cir. 1993); *Raytech Corp. v. White*, 54 F.3d 187, 190 (3rd Cir. 1995).

[142] *Use of Classified Information Order*, 44 Rad. Reg. 2d at 610, para. 6. With regard to the classified evidence in this case, the Commission has authority to protect classified evidence from release. 47 U.S.C. § 154(j). CTA would not be afforded access to it in any case. *See Jifry v. FAA*, 370 F.3d 1174, 1184 (D.C. Cir. 2004).

[143] CTA Mar. 1, 2021 Reply at 21 (citing, for example, *People's Mojahedin Org. v. U.S. Dep't of State*, 613 F.3d 220, 227 (D.C. Cir. 2010) (per curiam); *Holy Land Found. For Relief & Devel. v. Ashcroft*, 333 F.3d 156, 164 (D.C. Cir. 2003); *KindHearts for Charitable Humanitarian Dev., Inc. v. Geithner*, 710 F. Supp. 2d 637, 660 (N.D. Ohio 2010)). *See, e.g., Jifry*, 370 F.3d at 1183–84 (collecting cases).

[144] *Institution Order*, 35 FCC Rcd at 15012, para. 10 (citing 5 U.S.C. § 558(c)).

[145] 5 U.S.C. § 558(c).

been given multiple opportunities to address these concerns and has failed to do so."[146] Notably, CTA has not proffered any argument as to how it can address the Executive Branch agencies' and our fundamental concerns in this proceeding—namely, concerns over CTA's ownership and control by the Chinese government raising substantial and unacceptable national security and law enforcement risks related to its retention of its domestic section 214 authority and international section 214 authorizations that cannot be addressed through further mitigation with the Executive Branch agencies.

34. As an independent ground for our decision, we agree with the Executive Branch agencies that section 558(c)(2) of the APA "provides an exception to these requirements 'in cases of willfulness or those in which public health, interest, or safety requires otherwise.' The instances involving the public interest and safety are reflected by the national security and law enforcement risks posed by [CTA's] retention of international [s]ection 214 authorizations as articulated by the Executive Branch's submissions."[147] We also agree with the Executive Branch agencies that section 558(c) "prevents willfully noncompliant licensees, such as [CTA], from gaming the APA's procedural protections as a way to delay revocation without making good faith efforts to achieve compliance."[148]

35. As discussed below, separate and apart from our finding concerning revocation, we terminate CTA's international section 214 authorizations based on CTA's willful violation of two of the five provisions of the 2007 LOA, compliance with which is an express condition of CTA's international section 214 authorizations.[149] Among our findings, CTA's practice of knowingly {[ ]} without honoring its commitment to disclose this fact to the Executive Branch agencies, {[ ]} amounts to a willful violation of the requirement to take "all practicable measures" to prevent unauthorized access to U.S. records.[150] CTA also improperly redacted the 2018 U.S. Records Security Agreement so as to conceal the fact that {[ ]}[151]

36. CTA contends that the willfulness exception "requires engagement in a prohibited act, whether intentionally or though careless disregard of statutory requirements,"[152] and that it is CTA's

[146] *See* Executive Branch Response at 6. In essence, CTA has already had its "second chance" to achieve compliance, which, as the Court of Appeals for the Ninth Circuit observed, is the purpose of § 558(c). *Air North America v. Dep't of Transp.*, 937 F.2d 1427, 1438 (9th Cir. 1991).

[147] Executive Branch Response at 7.

[148] *Id*.

[149] 2007 LOA. *See infra* Section III.C. for a discussion of CTA's violations of the 2007 LOA.

[150] *See infra* Section III.C.; *see also infra* paras. 107-10; Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15, Responses of China Telecom (USA) Corporation Combined Questions for FCC Applicants (May 11, 2007) (May 11, 2007 Response); *id.*, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter from [CTA] to DOJ National Security Division, DHS and FBI (January 11, 2016 Letter); *id.*, Business Confidential Exh. 103 at EB-2111-12, Apr. 4, 2019 Letter from Morgan Lewis to DOJ National Security Division (April 4, 2019 Letter); *see* CTA June 8, 2020 Response, Exh. 16 at 28-29. *See also Institution Order*, 35 FCC Rcd at 15029-30, 15037-38, paras. 38-39, 54.

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

[151] Executive Branch Response at 7 & n.28 (citing Executive Branch Recommendation to Revoke and Terminate at 18, n.65 (citing *id.*, Business Confidential Exh. 37 at EB-655)). *See also* Executive Branch Recommendation to Revoke and Terminate at 18, 56 (quoting *id.*, Business Confidential Exh. 37 at EB-655); CTA June 8, 2020 Response, Exh. 16 at 22, n.40.

[152] CTA Mar. 1, 2021 Reply at 29 (emphasis omitted); *id*. at 27 (citing *Coosemans Specialties, Inc. v. Dep't of Agriculture*, 482 F.3d 560, 567 (D.C. Cir. 2007) (citing *Finer Foods Sales Co. v. Block*, 708 F.2d 774, 778 (D.C. Cir. 1983))).

"compliance with the terms of the LOA to which the 'willfulness' exception is relevant, not what may or may not have happened after the Executive Branch raised questions about 'potential breaches of the LOA[.]'"[153] We do not agree with CTA's argument that its actions following the Executive Branch agencies' notification of the breaches are not demonstrative of willfulness, and the record evidence indicates as such. The Act is instructive in this case. The Act provides that "[w]illfulness" in the section 312 context, upon which CTA otherwise relies, "when used with reference to the commission or omission of any act, means the conscious and deliberate commission or omission of such act, irrespective of any intent to violate any provision of this chapter or any rule or regulation of the Commission authorized by this chapter or by a treaty ratified by the United States."[154] In this regard, CTA has presented no evidence that its actions in violation of the 2007 LOA—compliance with which is a prerequisite for its international section 214 authorizations—were not conscious or deliberate. Importantly, there is record evidence to demonstrate willful behavior of a prohibited act.[155] Moreover, as the Commission stated in the *Institution Order*, in the context of the termination of CTA's international section 214 authorizations, section 558(c)(2) does not grant a substantive right to escape from a condition that terminates a license.[156]

37. CTA further argues that the question of whether it acted willfully "should have been designated for hearing,"[157] but "[n]othing in the [APA] imposes that requirement or supports the petitioner's apparent contention that the determination of willfulness itself may be made only after a hearing."[158] Moreover, nothing in the APA requires the application of trial-type procedures to the ensuing proceeding even when section 558 applies.[159]

38. Finally, even if the willfulness exception were not to apply, we conclude that the public interest exception would. Indeed, our conclusions about the national security imperatives here could have allowed the Commission to proceed immediately to a decision on whether to revoke CTA's section 214 authorizations on the existing record, without undertaking the additional process it has afforded here, on the basis that "public health, interest, or safety requires" doing so.[160] Certainly, now, having carefully reviewed the record, we conclude that those imperatives and the fiscal and administrative burden of additional process require a decision without additional delay or process.

[153] *Id.* at 29 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 102 at EB-2103).

[154] 47 U.S.C. § 312(f).

[155] *See infra* Section III.C. for a discussion of CTA's willful behavior of prohibited acts.

[156] *Institution Order*, 35 FCC Rcd at 15042, para. 61; *see, e.g.*, *Atlantic Richfield Co. v. United States*, 774 F.2d 1193, 1200-01 (D.C. Cir. 1985) (holding that the procedural requirements of section 558(c) apply only where "the licensee [may] be able to establish compliance with all legal requirements or . . . change its conduct in a manner that will put its house in lawful order" and noting that "[a] license that expires on its own terms is not protected by [section 558(c)]") (internal quotation and citations omitted).

[157] CTA Mar. 1, 2021 Reply at 29.

[158] *Finer Foods Sale Co. v. Block*, 708 F.2d 774, 778 (D.C. Cir. 1983).

[159] *Institution Order*, 35 FCC Rcd at 15015-16, para. 18, n.57 (citing *Empresa Cubana Exportadora de Alimentos y Productos Varios v. U.S. Dep't of the Treasury*, 638 F.3d 794, 802 (D.C. Cir. 2011) (citing *Gallagher & Ascher Co. v. Simon*, 687 F.2d 1067, 1073-75 (7th Cir. 1982) (collecting cases))).

[160] 5 U.S.C. § 558(c); *Institution Order*, 35 FCC Rcd at 15015, para. 18; *cf. China Unicom Americas Institution Order*, 36 FCC Rcd at 6330-31, para. 19 (observing that, especially "given the national-security issues at stake," the "fiscal and administrative burden" of additional procedures and the risk of "unwarranted delay" would support forgoing any unnecessary process).

d. No Material Facts in Dispute Warranting a Hearing

39. 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,[161] despite CTA's arguments that the Commission cannot avoid a hearing by claiming that no material facts are in dispute.[162] 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 otherwise. We find here that the question of whether revocation and termination is appropriate does not turn on disputed issues of fact, nor is the credibility of any material evidence in the record reasonably questioned. 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.

40. *First*, we disagree with CTA's assertion that by inviting parties to comment on the appropriate standard of proof, the Commission tacitly admitted the existence of material disputed facts that warrant an evidentiary hearing because "the standard of proof is only relevant if material facts remain disputed such that adjudication is necessary."[163] The Commission discussed and sought comment on the standard of proof in a footnote in the *Institution Order* to address CTA's argument that revocation "requires" a showing by clear and convincing evidence of egregious conduct.[164] The Commission explained 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."[165] The Commission's subsequent invitation for "parties to address this question further in their subsequent filings"[166] was not an acknowledgment—tacit or otherwise—that there were material facts in dispute, but was intended to allow parties an additional opportunity to comment on and develop the record on this legal issue. Indeed, this approach is consistent with the procedures the Commission adopted in the *Institution Order* affording CTA the further opportunity to respond to the serious national security and law enforcement concerns raised regarding its section 214 authority.

41. *Second*, we are not persuaded by CTA's bare assertion that "there is an abundance of material facts that remain in dispute"[167] regarding the allegations in the Executive Branch Recommendation to Revoke and Terminate in relation to the requirements of the 2007 LOA and CTA's compliance therewith, CTA's statements to the Executive Branch agencies, and the Executive Branch agencies' understanding of Chinese law, among others.[168] As discussed below, CTA's "disputes" amount to a summary of its ultimate legal contentions in this case; the underlying facts are undisputed or have been developed through a written record. These include whether CTA violated its obligations under the 2007 LOA and failed to disclose to U.S. government authorities critical information regarding the location of its U.S. records, among other things. The disputes here, as we observed in a similar case, "do not turn on witnesses testifying to their personal knowledge or observations or on individual credibility

[161] *Institution Order*, 35 FCC Rcd at 15015, para 17.

[162] CTA Mar. 1, 2021 Reply at 29; CTA June 8, 2020, Response at 6.

[163] CTA Mar. 1, 2021 Reply at 30.

[164] CTA June 8, 2020 Response at 8; *Institution Order*, 35 FCC Rcd at 15014, para. 15, n.49.

[165] *Institution Order*, 35 FCC Rcd at 15014, para. 15, n.49.

[166] *Id*.

[167] CTA Mar. 1, 2021 Reply at 33. CTA also states that "[e]ven assuming *arguendo* that the record contains sufficient evidence to support the Commission's apparent findings on these issues (which CTA does not admit), it is utterly incredible to assert that this evidence is undisputed." *Id*.

[168] *Id*. at 30.

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 [the section 214 authorization holder's] ultimate ownership and control by the Chinese government."[169] Nothing in any of the filings by CTA, before or after the *Institution Order*, identifies any such substantial and material issues of fact, much less those that require credibility determinations.

42. We agree with the Executive Branch agencies' observation that "[w]hether the [Chinese] government controls [CTA] can be decided by the Commission based on facts already in the record."[170] This is also the case with issues related to CTA's compliance with the LOA, its statements to the Executive Branch agencies, and the interpretation of Chinese laws. None of CTA's contentions calls into question the Commission's preliminary view in the *Institution Order*, based on the partial record before it then, that these matters do not "warrant[] an adjudicatory hearing before an Administrative Law Judge or other presiding officer."[171] As discussed below, nothing in the current record as a whole indicates that CTA requires an administrative hearing to meaningfully present its case and that it cannot do so through its written submissions, including its contentions that the allegations against it rely on "misrepresentations of fact."[172] More importantly, CTA provides no additional evidence, apart from its responses to the record evidence introduced by the Executive Branch agencies, to support its claims that "the picture presented by the Executive Branch is not accurate or, in other cases, lacks context."[173]

43. We are also not persuaded by CTA's argument that the Commission "cannot escape the requirements of a hearing by contending it can decide this case solely on the basis of those facts that are not disputed, such as CTA's corporate structure and ultimate ownership, and dismissing all other factual disputes as 'immaterial' to its decision"[174] 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."[175] Nor do we find persuasive the argument that "to the extent the Commission seeks to rely on allegations about CTA's trustworthiness resulting from alleged past conduct and representations to the Executive Branch, those issues are facts that must be assessed through an evidentiary hearing process"[176] since "[q]uestions of intent are factual[.]"[177] Contrary to CTA's claim, as

[169] *China Unicom Americas Institution Order*, 36 FCC Rcd at 6331-32, para. 21.

[170] Executive Branch Response at 9. Indeed, the evidence supporting the Executive Branch Recommendation to Revoke and Terminate "includes many of CTA's own documents that were voluntarily provided to the Executive Branch. CTA has not objected to the inclusion of this evidence in the record. It even cites Executive Branch exhibits (more than 50 times) in the Response to support its own arguments." *Id*. at 8.

[171] *Institution Order*, 35 FCC Rcd at 15015, para 17.

[172] CTA Mar. 1, 2021 Reply at 16; *see also id.* at 21, 23.

[173] *Id*. at 37.

[174] *Id*. at 33.

[175] *Id*.; *see id* at 33-36 (distinguishing, as support for its arguments that a hearing is warranted on the facts alleged to justify revocation, *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). We are not persuaded that these cases support CTA'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 CTA." *Id*. at 34. 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). 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.

[176] CTA Mar. 1, 2021 Reply at 32.

explained above, intent is not required by the Act to prove willfulness, only "the conscious and deliberate commission or omission of such act, irrespective of any intent . . . ."[178] Again, the matters under consideration here do not turn on witnesses testifying to their personal knowledge or observations or on individual credibility determinations, for example, but instead on facts that can be fully ascertained through written evidence and on national security and law enforcement concerns associated with CTA's ultimate ownership and control by the Chinese government. And CTA has offered no new evidence that would dispel the Commission's prior analysis in the *Institution Order* as discussed in detail below.[179] Finally, we find that the Commission is exercising its well-established discretion[180] to proceed without holding an evidentiary hearing, and we base our decision today on the overall assessment of the public interest.

B. Revocation of Section 214 Authority

44. Based on our public interest analysis under section 214 of the Act and the totality of the extensive unclassified record evidence alone, we find that the present and future public interest, convenience, and necessity is no longer served by CTA's retention of its section 214 authority, and we revoke CTA's domestic and international section 214 authority.[181] We find that CTA, 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. CTA's ownership and control by the Chinese government raise significant national security and law enforcement risks by providing opportunities for CTA and Chinese state-sponsored actors to access, store, disrupt, and/or misroute U.S. communications, which in turn allow them to engage in espionage and other harmful activities against the United States. Given the changed national security environment with respect to China since the Commission authorized CTA to provide telecommunications services in the United States, we find that CTA's ties to the Chinese government—together with Chinese laws obligating CTA and its direct and indirect parent entities and affiliates to cooperate with requests by the Chinese government—pose a clear and imminent threat to the security of the United States due to CTA's access to U.S. telecommunications infrastructure.[182] We find that these risks cannot be addressed through further mitigation with the Executive Branch agencies. Additionally, although it is not necessary to support these findings and

(Continued from previous page)

[177] *Id*. at 37 (citing *California Public Broadcasting Forum v. FCC*, 752 F.2d 670, 679 (D.C. Cir. 1985) (citing *Pullman-Standard v. Swint*, 456 U.S. 273, 278 (1982) ("Treating issues of intent as factual matters for the trier of fact is commonplace.")). CTA argues that "[t]he D.C. Circuit has required an evidentiary hearing in cases where the only conflicting facts centered around statements made to third parties. Here, the Commission is seeking to rely on assertions about CTA's interactions with third parties, at least in part, to revoke (or terminate) CTA's [s]ection 214 authorizations, and CTA has put forward substantial evidence that the picture presented by the Executive Branch is not accurate or, in other cases, lacks context." *Id*. CTA also argues that "the Commission must at a minimum conduct a hearing to determine which version of events as to CTA's interactions with the Executive Branch is the true and correct one." *Id.* We are not persuaded by CTA's arguments. In our judgment, there is nothing to be gained from subjecting officials from Executive Branch agencies to cross-examination; no substantial and material facts could be resolved by holding further proceedings, and the value of any further proceedings would be substantially outweighed by the harms.

[178] *See supra* para. 36; 47 U.S.C. § 312(f).

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

[180] *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.").

[181] *See generally Institution Order.*

[182] *See id*., 35 FCC Rcd at 15016-17, para. 20; *see also Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, 11442, paras. 27, 49.

conclusions, we find that the classified evidence submitted by the Executive Branch agencies further supports our decisions here.[183]

1. The Chinese Government Indirectly Owns and Controls CTA

45. The record is clear that CTA is "wholly owned and controlled by a single Chinese entity," CTCL, which is majority-owned and controlled by CT, a Chinese state-owned enterprise, and therefore CTA is subject to exploitation, influence, and control by the Chinese government.[184] Significantly, in January 2018, CTCL revised its Articles of Association to give the Chinese Communist Party greater control over the management and operations of its business.[185] The record evidence supports the Executive Branch agencies' assessment that "[t]he Chinese government's controls over the Parent Entity [CTCL] and [CTA], combined with newly enacted Chinese laws, raise significant concerns that [CTA] will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests,"[186] and we find nothing in the record to rebut these concerns. These laws include the Cybersecurity Law of the People's Republic of China, effective June 1, 2017 (2017 Cybersecurity Law),[187] the implementing regulation for the Cybersecurity Law, effective November 1, 2018 (2018 Cybersecurity Regulation),[188] and the National Intelligence Law of the P.R.C., effective June 28, 2017 (2017 National Intelligence Law).[189] Indeed, the

[183] *See infra* Section III.E.

[184] *Institution Order*, 35 FCC Rcd at 15017, para. 22; Executive Branch Recommendation to Revoke and Terminate at 34.

[185] *Institution Order*, 35 FCC Rcd at 15017-18, para. 22; Executive Branch Recommendation to Revoke and Terminate at 36 (citing *id.*, Exh. 48 at EB-735 and EB-766, China Telecom Corp. Ltd., Annual Report (Form 20-F) (Apr. 27, 2018), Exh. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018 (CTCL Apr. 27, 2018 Form 20-F) (Articles 9 and 98 of unofficial English translation of Articles of Association as filed with the SEC on Apr. 27, 2018 as part of Annual Report (Form 20-F)); *id.*, Exh. 114 at EB-2404, 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)).

[186] Executive Branch Recommendation to Revoke and Terminate at 38; *see also id.* at 38-40; *Institution Order*, 35 FCC Rcd at 15018, para. 22.

[187] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 38-39; *id.*, Exh. 51 at EB-866, Translation: Cybersecurity Law of the People's Republic of China (Passed November 6, 2016 and effective June 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/; *id.*, Exh. 53 at EB-901, *China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*, Library of Congress, http://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-inspection-powers-issued/ (Nov. 13, 2018) (*China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*); *see* The National People's Congress of the People's Republic of China, *Cybersecurity Law of the People's Republic of China*, http://www.xinhuanet.com//politics/2016-11/07/c_1119867015 htm (last visited Oct. 4, 2021).

[188] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 39 (stating, "[t]he November 1, 2018 'Regulation on Internet Security Supervision by Public Security Organs' (Order No. 151 of the Ministry of Public Security) provided further directives for implementing the 2017 Cybersecurity Law.") (citing *id.*, Exh. 53 at EB-901, *China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*; *id.*, Exh. 54 at EB-903, *China's New Cybersecurity Measures Allow State Police to Remotely Access Company Systems*, Recorded Future Blog (Feb. 8, 2019), https://www.recordedfuture.com/china-cybersecurity-measures/); *see Regulation on Internet Security Supervision by Public Security Organs*, http://www.gov.cn/gongbao/content/2018/content_5343745.htm (last visited Oct. 4, 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 Oct. 4, 2021).

[189] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 35 & n.123; *id.*, Exh. 118 at EB-2735, China Law Translate, National Intelligence Law of the P.R.C. (2017) (Passed on June 27, 2017 and effective June 28, 2017), https://www.chinalawtranslate.com/en/national-intelligence-

(continued….)

former U.S. National Security Advisor cautioned about "the integrated nature of the Chinese Communist Party's military and economic strategies," adding that the Chinese Communist Party "is obsessed with control—both internally and externally," and that under Article 7 of the 2017 National Intelligence Law, "all Chinese companies must collaborate in gathering intelligence."[190] As stated in the *Institution Order*, "'the Chinese government is highly centralized and exercises strong control over commercial entities, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information.'"[191]

46. CTA asserts, however, that "CTA operates its U.S. business as an independent corporation that runs on a day-to-day basis under the direction of its own local managers on core business matters"[192] and "CTA's owners do not actively direct CTA's daily operations."[193] CTA further states that it "exists and operates as an independent business that would be able to serve its customers without CTCL (*e.g.*, by engaging in similar agreements with other carriers) . . . ."[194] CTA emphasizes that it "maintains control of its day-to-day operations without interference by CTCL or any other entity,"[195] and that "CTA and CTCL do not share identical officers, directors, or senior management officials."[196] We are not persuaded by these arguments.

47. Contrary to CTA's arguments, the record demonstrates that CTA is not independent and its parent entities, CTCL and CT, have the ability to exercise significant and substantial influence and control over CTA. The evidence overwhelmingly supports the Executive Branch agencies' assessment that, "[b]y controlling the board, [CTCL] also controls [CTA's] ability to set fundamental policies, finances, budgets, and long term strategic plans."[197] Likewise, CT, a state-owned enterprise that is directly and wholly owned and controlled by the Chinese government, has the ability to influence CTA,[198]

(Continued from previous page)
law-of-the-p-r-c-2017/; *id.*, Exh. 120 at EB-2747, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare Blog, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (July 20, 2017) (*Beijing's New National Intelligence Law*); *see* The National People's Congress of the People's Republic of China, *National Intelligence Law of the People's Republic of China*, http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm (last visited Oct. 4, 2021). *See also* Executive Branch Recommendation to Revoke and Terminate, Exh. 114 at EB-2384, Revised Constitution.

[190] *Institution Order*, 35 FCC Rcd at 15018, para. 22; H.R. McMaster, *What China Wants*, The Atlantic, May 2020, at 70, 71, 72-73 (*What China Wants*), *available at* https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/.

[191] *Institution Order*, 35 FCC Rcd at 15022, para. 27 (quoting *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, para. 46 and citing *What China Wants* at 69-74).

[192] CTA Mar. 1, 2021 Reply at 48; *see also* CTA June 8, 2020 Response, Exh. 3 at 1, 4; *Institution Order*, 35 FCC Rcd at 15022, para. 28.

[193] CTA Mar. 1, 2021 Reply at 48; *see also* CTA June 8, 2020 Response, Exh. 3 at 1, 4; *Institution Order*, 35 FCC Rcd at 15022, para. 28.

[194] CTA Mar. 1, 2021 Reply at 48.

[195] *Id*. at 49; *see also* CTA June 8, 2020 Response, Exh. 3 at 1.

[196] CTA Mar. 1, 2021 Reply at 47 (citing CTA June 8, 2020 Response, Exhs. 4, 5).

[197] Executive Branch Response at 10 (citing CTA June 8, 2020 Response, Exh. 3).

[198] *See* CTA June 8, 2020 Response, Exhs. 1, 1-1, 2; Executive Branch Recommendation to Revoke and Terminate at 32-37; *Institution Order*, 35 FCC Rcd at 15021, para. 25 & n.97.

as the corporate leadership of CTCL includes individuals comprising the corporate leadership of CT as discussed below.[199]

48. CTA's claims that it operates as an independent business are further undermined by CTA's admission in its June 8, 2020 Response that "CTCL, as CTA's direct parent and sole shareholder, reviews and approves certain major decisions."[200] In particular, CTA states that its "[b]ylaws authorize CTCL, as the sole stockholder of CTA, to examine the Board's reports, . . . approve and amend CTA's core institutional documents, and approve other major matters which are subject to the approval of stockholders" and that "CTCL may also authorize or delegate to the Board to carry out such matters."[201] CTA also states that "[a]s the sole stockholder in CTA, CTCL has the power to elect, remove and replace directors."[202] Furthermore, {[

]}[204] Notably, CTA did not disclose these facts to the Commission in its June 8, 2020 filing.

49. Moreover, CTA's June 8, 2020 Response indicated that {[

]}[205] Based

[199] China Telecom Corporation Limited, *Board of Directors and Senior Executives*, https://www.chinatelecom-h.com/en/company/executives.php (last visited Oct. 4, 2021) (CTCL Board of Directors and Senior Executives); China Telecom Corporation Limited, *Board of Directors and Senior Executives—Mr. Ke Ruiwen*, https://www.chinatelecom-h.com/en/company/bio.php?from=directors&id=keruiwen (last visited Oct. 4, 2021); China Telecom Corporation Limited, *Board of Directors and Senior Executives—Mr. Li Zhengmao*, https://www.chinatelecom-h.com/en/company/bio.php?from=directors&id=lizhengmao (last visited Oct. 4, 2021); China Telecom Corporation Limited, *Board of Directors and Senior Executives—Mr. Shao Guanglu*, https://www.chinatelecom-h.com/en/company/bio.php?from=directors&id=shaoguanglu (last visited Oct. 4, 2021) (*Board of Directors and Senior Executives—Mr. Shao Guanglu*); China Telecom Corporation Limited, *Board of Directors and Senior Executives—Mr. Liu Guiqing*, https://www.chinatelecom-h.com/en/company/bio.php?from=directors&id=liuguiqing last visited Oct. 4, 2021); China Telecom Corporation Limited, *Board of Directors and Senior Executives—Madam Zhu Min*, https://www.chinatelecom-h.com/en/company/bio.php?from=directors&id=zhumin last (visited Oct. 4, 2021); *see* China Telecom Corporation Limited, Annual Report 2020 at 19-21 (2021), https://www.chinatelecom-h.com/en/ir/report/annual2020.pdf (CTCL Annual Report 2020); *see infra* para. 49. *See also* CTA June 8, 2020 Response, Exh. 5; *Institution Order*, 35 FCC Rcd at 15023, para. 28.

[200] CTA June 8, 2020 Response, Exh. 3 at 1.

[201] *Id*., Exh. 3 at 2; *Institution Order*, 35 FCC Rcd at 15022, para. 28.

[202] CTA June 8, 2020 Response, Exh. 3 at 2.

[203] *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-590, EB-638-641, Dec. 6, 2018 Letter from Morgan Lewis to DOJ National Security Division with attachments (December 6, 2018 Letter with Attachments).

[204] *Id.*, Business Confidential Exh. 36 at EB-639, December 6, 2018 Letter with Attachments. {

]} *Id.*

[205] CTA June 8, 2020 Response, Exh. 5; *Institution Order*, 35 FCC Rcd at 15023, para. 28. Based on CTA's June 8, 2020 Response, {[ ]} individuals identified as the officers and directors of CTCL (including all individuals identified as an officer and/or {[

(continued….)

on publicly available information associated with CTCL, three individuals identified in CTA's June 8, 2020 filing as directors and/or officers of CTCL {[ ]} no longer hold those positions at CTCL.[206] However, other corporate governance information associated with CTCL in CTA's filing remains unchanged as of September 30, 2021.[207] Importantly, the record shows that the Chairman and Chief Executive Officer of CTCL is also the Chairman of CT.[208] The President and Chief Operating Officer of CTCL is also the President of CT.[209] In addition, three of the individuals identified as a {[ ]} of CTA's Board of Directors are identified as {[

]}[211]

(Continued from previous page) ———————————

]} CTA June 8, 2020 Response, Exh. 5; *Institution Order*, 35 FCC Rcd at 15023, para. 28, n.109.

[206] Based on CTCL's publicly available information, three individuals identified in CTA's June 8, 2020 filing as "Executive Director and Executive Vice President," "Executive Director and Executive Vice President," and "Executive Vice President" of CTCL {[ ]} no longer hold these positions at CTCL as of December 2020, January 2021, and September 2021, respectively. *See, e.g.*, China Telecom Corporation Limited, Report of Foreign Private Issuer (Form 6-K), Exh. 1.1 at 10-12, Poll Results of Annual General Meeting, Appointment and Change Of Directors and Supervisors and Payment of the Final Dividend (May 27, 2020), https://www.sec.gov/Archives/edgar/data/1191255/000119312520151699/d934058d6k htm#toc (identifying the Board of Directors of CTCL as at the date of the announcement on May 26, 2020) (CTCL May 27, 2020 Form 6-K); *id.*, Exh. 1.2 at 1, List of Directors and Their Role and Function; China Telecom Corporation Limited, Annual Report (Form 20-F) at 54-55 (Apr. 28, 2021), https://www.sec.gov/Archives/edgar/data/1191255/000119312521135257/d38433d20f.htm ("Directors and Senior Officers"); China Telecom Corporation Limited, Resignation of Director and Change of Important Executive Position (Dec. 4, 2020), https://doc.irasia.com/listco/hk/chinatelecom/announcement/a201204.pdf; China Telecom Corporation Limited, Resignation of Director and Change of Important Executive Position (Jan. 19, 2021), https://doc.irasia.com/listco/hk/chinatelecom/announcement/a210119.pdf; China Telecom Corporation Limited, Change of Important Executive Position (Sept. 30, 2021), https://doc.irasia.com/listco/hk/chinatelecom/announcement/a210930.pdf (Sept. 30, 2021 Announcement). *See also* CTA June 8, 2020 Response, Exh. 5.

[207] *Sept. 30, 2021 Announcement*; *CTCL Board of Directors and Senior Executives*; China Telecom Corporation Limited, *Board of Directors*, https://www.chinatelecom-h.com/en/cg/directors.php (last visited Oct. 4, 2021) (CTCL Board of Directors). *See also* CTA June 8, 2020 Response, Exh. 5. In its June 8, 2020 Response, CTA {[

]} *See* CTA June 8, 2020 Response, Exh. 5. We note that CTCL's publicly available information, including information as of May 26, 2020 and as of year-end 2020 or afterwards, identifies one of the members of its Board of Directors, {[ ]} as "a Deputy Director of Communications Science and Technology Committee of the Ministry of Industry and Information Technology of the People's Republic of China." *See* CTA June 8, 2020 Response, Exh. 5 at 3, 8; *Board of Directors and Senior Executives—Mr. Shao Guanglu*; CTCL Annual Report 2020 at 20, 51-52; CTCL May 27, 2020 Form 6-K, Exh. 1-1 at 10-11.

[208] CTCL Annual Report 2020 at 18-19; *CTCL Board of Directors and Senior Executives*; *CTCL Board of Directors*. *See also* CTA June 8, 2020 Response, Exh. 5 at 1, 7; *Institution Order*, 35 FCC Rcd at 15023, para. 28.

[209] CTCL Annual Report 2020 at 19; *CTCL Board of Directors and Senior Executives*; *CTCL Board of Directors*. *See also* CTA June 8, 2020 Response, Exh. 5 at 1-2, 8; *Institution Order*, 35 FCC Rcd at 15023, para. 28.

[210] CTA June 8, 2020 Response, Exh. 4; *Institution Order*, 35 FCC Rcd at 15022-23, para. 28. {[ ]} CTA June 8, 2020 Response, Exh. 4 at 4-5.

[211] Executive Branch Recommendation to Revoke and Terminate at 24; *id.*, Exh. 4 at EB-63, EB-67, China Telecom Corp. Ltd., Annual Report Form 20-F (Apr. 27, 2018) (CTCL Apr. 27. 2018 Form 20-F).

50. Further, the record evidence shows that other important matters are overseen {[

]}[212] Previously, in an October 1, 2018 Letter responding to questions in the Executive Branch agencies' June 13, 2018 Letter, CTA stated that {[

]}[214] According to the June 9, 2020 Senate Permanent Subcommittee on Investigations (Senate Subcommittee) Staff Report titled, "Threats to U.S. Networks: Oversight of Chinese Government-Owned Carriers" (PSI Report), CTA informed Team Telecom during the agencies' site visit on March 10, 2017, "that its budget was subject to approval" by CTG and that CTA also consulted with CTG on technical matters that relate to the establishment of network points of presence within the United States.[215]

51. In addition to the presence of identical officers and directors associated with CTA's direct and indirect parent entities, {[

]}[216] Based on CTA's June 8, 2020 Response and publicly

[212] *Id.*, Business Confidential Exh. 36 at EB-640, December 6, 2018 Letter with Attachments. {

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-640 (emphasis added).

[213] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 92 at EB-1983, EB-1985, Oct. 1, 2018 Letter from Morgan Lewis to DOJ National Security Division (October 1, 2018 Letter); CTA June 8, 2020, Exh. 16 at 26, 39-40.

[214] *Id.*, Business Confidential Exh. 92 at EB-1985, October 1, 2018 Letter.

[215] Executive Branch Response, Exh. 128 at EB-2971, 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* at 63 (June 9, 2020), https://www.hsgac.senate.gov/imo/media/doc/2020-06-09%20PSI%20Staff%20Report%20-%20Threats%20to%20U.S.%20Communications%20Networks.pdf (PSI Report) (citations omitted). According to the PSI Report, CTA noted that it established "'a [new] Dallas [point of presence]' after 'discussion' with CTG." *Id.* (citations omitted).

[216] *See supra* paras. 47, 49; *see also* CTA June 8, 2020 Response, Exhs. 4, 5; *Institution Order*, 35 FCC Rcd at 15019, 15023, paras. 23, 28.

available information about CTCL's current leadership, CTA's corporate governance information shows that the officers and directors of CTCL who are not {[ ]}[217] Additionally, all officers and directors of CT are {[ ]}[218] The record shows that three of the individuals who are identified as a {[ ]} of CTA's Board of Directors are {[ ]}[219] As discussed below, CTA has provided no evidence to dispel the significance of {[ ]}

52. We reject CTA's argument that "CTCL'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."[220] As an initial matter, the full statement by the Commission that CTA cites for this assertion refers to "the minority shareholder," an important omission that CTA neglects to clarify.[221] We do not accept CTA's suggestion that CTCL should be viewed as a minority shareholder of CTA when CTA expressly states that CTCL holds 100% direct ownership of CTA.[222] Indeed, in its June 8, 2020 Response, CTA refers several times to CTCL as its "sole stockholder," stating, "as the sole stockholder, CTA's immediate corporate parent, CTCL oversees and approves certain major decisions, including decisions on significant expenditures, projects, investments, and other commercial obligations."[223] Additionally, {[ ]}[225]

53. We also reject CTA's argument that because it "is a Delaware corporation that is subject to U.S. law, [it is] not 'subject to the exploitation, influence, and control of the Chinese government.'"[226]

---

[217] CTA June 8, 2020 Response, Exh. 5; *Institution Order*, 35 FCC Rcd at 15019, para. 23; *see supra* para. 49.

[218] CTA June 8, 2020 Response, Exh. 5; *Institution Order*, 35 FCC Rcd at 15019, para. 23.

[219] CTA June 8, 2020 Response, Exh. 4; *Institution Order*, 35 FCC Rcd at 15019, para. 23.

[220] CTA Mar. 1, 2021 Reply at 49.

[221] *Id*. (citing *Baker Creek Communications, LLC* [sic], Memorandum Opinion and Order, 13 FCC Rcd 18709, 18714-15, para. 9 (1998) and quoting from that 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'"). CTA omits the Commission's reference in the quoted statement to "minority shareholder." The 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." *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 (1998) (emphasis added).

[222] CTA June 8, 2021 Response, Exh. 1 at 1; *id.*, Exh. 1-1.

[223] *Id*., Exh. 3 at 1.

[224] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621, December 6, 2018 Letter with Attachments.

[225] *Id*., Business Confidential Exh. 36 at EB-622, December 6, 2018 Letter with Attachments. {

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621.

[226] CTA June 8, 2020 Response at 2; *Institution Order*, 35 FCC Rcd at 15021-22, paras. 26-27. CTA further contends that "the Commission agrees with the Executive Branch that CTA is controlled by the [Chinese] government and its existence as a separate corporate entity should be disregarded" and "[s]uch a speculation runs (continued….)

The Commission found unpersuasive a similar argument in the *China Mobile USA Order*,[227] noting therein that "[t]he Executive Branch agencies' assessment that China Mobile USA is subject to influence and control by the Chinese government is supported by our understanding that Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world."[228] 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." CTA also fails to refute the significant concerns presented by Chinese laws as discussed below. Additionally, the finding that we make in this Order—that, due to its ultimate ownership, CTA is subject to exploitation, influence, and control by the Chinese government—is not reliant on piercing the corporate veil.[229] Our finding is based on the public interest analysis under section 214 of the Act, taking into account the significant and substantial national security and law enforcement concerns associated with CTA's ultimate ownership and control by the Chinese government.

54. Additionally, we find that the Chinese government has the ability to exercise influence and control over CTA's direct parent entity, CTCL, and consequently CTA, through CTCL's amendments to its Articles of Association in January 2018 that give the Chinese Communist Party significant controls over CTCL's management and operations.[230] In the *Institution Order*, the Commission stated that "with respect to changes to [CTCL's] Articles of Association . . . these amendments signify the Chinese government's ability to influence state-owned enterprises, and consequently their indirect subsidiaries."[231] According to the Executive Branch agencies, in January 2018, CTCL revised Articles 9 and 98 of its Articles of Association "three months after the Chinese government amended the Constitution of the [Chinese Communist Party]," to conform to the constitutional amendments.[232] We note that the identical language in Article 98 of CTCL's 2018 Articles of Association is currently reflected in Article 129 of CTCL's Articles of Association that was amended

(Continued from previous page)
counter to CTA's legal status as a profit-making, commercial enterprise governed by the General Corporation Law of the State of Delaware that operates independently and without interference from its parent company." CTA Mar. 1, 2021 Reply at 32 (citing CTA June 8, 2020 Response, Exh. 3 at 1, 4; *id.*, Exh. 15 at 2-3, 5-6); *Institution Order*, 35 FCC Rcd at 15021-22, para. 26.

[227] *Institution Order*, 35 FCC Rcd at 15022, para. 27 (citing *China Mobile USA Order*, 34 FCC Rcd at 3371, para. 19; *id.* at 3376, para. 32, n.96 ("China Mobile USA argues that, as a Delaware corporation, it is 'subject to U.S. law' and the Chinese government's ownership and control of it would therefore not require it 'to comply with foreign government requests relating to its operations within the United States.'")).

[228] *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17; *Institution Order*, 35 FCC Rcd at 15022, para. 27 (quoting *China Mobile USA Order*, 34 FCC Rcd at 3369, para. 17).

[229] CTA Mar. 1, 2021 Reply at 45-51; Executive Branch Response at 9. Further, we are unpersuaded by CTA's contention that "even if the Executive Branch had alleged sufficient facts here to justify a veil-piercing inquiry, which it has not, under Commission precedent this issue would have to be designated for hearing before a neutral adjudicator." CTA Mar. 1, 2021 Reply at 45, n.163.

[230] *Institution Order*, 35 FCC Rcd at 15017-18, at para. 22; Executive Branch Recommendation to Revoke and Terminate at 36 (citing *id.*, Exh. 48 at EB-735 and EB-766, CTCL Apr. 27, 2018 Form 20-F, Exh. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018 (Articles 9 and 98 of unofficial English translation of Articles of Association as filed with the SEC on Apr. 27, 2018 as part of Annual Report (Form 20-F)); *id.*, Exh. 114 at EB-2404, Revised Constitution).

[231] *Institution Order*, 35 FCC Rcd at 15018-19, para. 23.

[232] Executive Branch Recommendation to Revoke and Terminate at 36 (citing *id.*, Exh. 114 at EB-2404, Revised Constitution; *id.*, Exh. 48 at EB-735 and EB-766, CTCL Apr. 27, 2018 Form 20-F, Exh. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018 (Articles 9 and 98 of unofficial English translation of Articles of Association as filed with the SEC on Apr. 27, 2018 as part of Annual Report (Form 20-F))).

and published on August 20, 2021.[233] The Revised Constitution of the Communist Party of China (Revised Constitution), revised and adopted on October 24, 2017 at the 19th National Congress of the Communist Party of China, states 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."[234]

55. In line with the Revised Constitution, Article 9 of CTCL's amended Articles of Association states that, "[i]n accordance with the Company Law and the Constitution of the Communist Party of China (the 'Party'), the Company shall set up Party organisations. *The Party organisations shall perform the core leadership and political functions.* The Company shall set up Party working organs, which shall be equipped with sufficient staff to handle Party affairs and provided with sufficient funds to operate the Party organisations."[235] Moreover, Article 129 of CTCL's amended Articles of Association states that, "[p]rior to making decisions on material issues of the Company, *the board of directors shall seek advice from the Party organisations.* When the board of directors appoints senior management personnel of the Company, the Party organisations shall consider and provide comments on the candidates for management positions nominated by the board of directors or the general manager, or recommend candidates to the board of directors and/or the general manager."[236] The changes are significant because, as noted by the Executive Branch agencies, prior to the January 2018 amendments, CTCL's Articles of Association did not mention the Chinese Communist Party.[237]

56. CTA disputes the importance of this evidence in its March 1, 2021 Reply, stating that while "[b]oth the Executive Branch and the Order Instituting Proceedings place great weight on amendments to CTCL's Articles of Association regarding the role of the Party organization within

[233] *See id.*, Exh. 48 at EB-766, CTCL Apr. 27, 2018 Form 20-F, Exh. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018; CTCL Aug. 20, 2021 Form 6-K, Exh. 1.1 at 48, Articles of Association of CTCL as of Aug. 20, 2021, Article 129.

[234] Executive Branch Recommendation to Revoke and Terminate, Exh. 114 at EB-2404, Revised Constitution, Article 33; *id.*, Exh. 114 at EB-2384; *Institution Order*, 35 FCC Rcd at 15018-19, para. 23 & n.80; *see also infra* para. 59 & note 255. Article 32 of the Revised Constitution states that "[p]rimary-level Party organizations play a key role for the Party in the basic units of social organization" and that their "main tasks" include "to encourage Party members and the people to consciously resist unacceptable practices and resolutely fight against all violations of Party discipline or state law." Executive Branch Recommendation to Revoke and Terminate, Exh. 114 at EB-2403-04, Revised Constitution, Article 32.

[235] Executive Branch Recommendation to Revoke and Terminate, Exh. 48 at EB-735, CTCL Apr. 27, 2018 Form 20-F, Exh. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018 (emphasis added); *id.* at 36-37; *Institution Order*, 35 FCC Rcd at 15019, para. 23. As we noted in a similar case, "Article 19 of the Company Law of the People's Republic of China (2018 Amendment) states, '[t]he Chinese Communist Party may, according to the Constitution of the Chinese Communist Party, establish its branches in companies to carry out activities of the Chinese Communist Party. The company shall provide necessary conditions to facilitate the activities of the Party.'" *Pacific Networks/ComNet Institution Order*, 36 FCC Rcd at 6389, n.142 (citing Law of China, Company Law of the People's Republic of China (2018 Amendment) at Article 19, http://lawinfochina.com/display.aspx?id=e797dd968c30e172bdfb&lib=law).

[236] CTCL Aug. 20, 2021 Form 6-K, Exh. 1.1 at 48, Articles of Association of CTCL as of Aug. 20, 2021, Article 129; Executive Branch Recommendation to Revoke and Terminate, Exh. 48 at EB-766, CTCL Apr. 27, 2018 Form 20-F, Ex. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018 (emphasis added); *id.* at 36-37; *Institution Order*, 35 FCC Rcd at 15019, para. 23.

[237] Executive Branch Recommendation to Revoke and Terminate at 37 (comparing *id.*, Exh. 49 at EB-798, China Telecom Corp. Ltd., Annual Report (Form 20-F) (Apr. 28, 2016), Exh. 1.1 (Articles of Association of China Telecom Corp. Ltd. as of May 27, 2015) with *id.*, Exh. 48 at EB-732, CTCL Apr. 27, 2018 Form 20-F, Exh. 1.1, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018).

CTCL,"[238] these amendments "were introduced only in the broader context of the Chinese government's reform of supervision and management of state-owned assets."[239] CTA contends that "[t]he amendments focused on capital management, and investors recognized these amendments as increasing the clarity and transparency of the role of Party organization while giving state-owned enterprises more independence from the Chinese government."[240]

57. CTA, however, provides no supporting evidence for these claims.[241] Indeed, CTA again does not dispute that the amendments to CTCL's Articles of Association confer express powers to Chinese Communist Party organizations within CTCL.[242] Furthermore, CTA's contention that the amendments "increas[e] the clarity and transparency of the role of Party organization while giving state-owned enterprises more independence from the Chinese government"[243] is contradicted by the record evidence concerning the plain language of CTCL's amended Articles of Association. The language of these amendments is clearly consistent with the Revised Constitution and ultimately gives the Chinese Communist Party greater control over the management and business operations of CTCL, CTA's direct parent entity, and therefore influence and control over CTA.

58. CTA contends that, "in any event, CTCL is not the entity that holds a Commission authorization,"[244] and asserts that "CTA's articles of incorporation and by-laws that govern its activities in the U.S. contain no references to any foreign government, any of its agencies, or any foreign political party."[245] These arguments do not squarely address the concerns raised by the Commission regarding, among other things, how changes to CTCL's Articles of Association signify the Chinese government's ability to influence state-owned enterprises, and consequently, their direct and indirect subsidiaries.[246] CTCL's amended Articles of Association raises serious concerns that the changes amplify the Chinese government's influence over CTCL, and consequently, CTA. CTA has not provided any evidence to the contrary. These concerns are reinforced by USTR's 2018 Report to Congress on China's WTO Compliance, which states, "the Party has taken further steps to increase the strength and presence of Party

[238] CTA Mar. 1, 2021 Reply at 49-50 (citing Executive Branch Recommendation to Revoke and Terminate at 36-37; *Institution Order*, 35 FCC Rcd at 15017-18, paras. 22-23).

[239] *Id*. (citing CTA June 8, 2020 Response, Exh. 15 at 5).

[240] *Id*. at 50 (citing CTA June 8, 2020 Response, Exh. 15 at 5).

[241] CTA does not provide or cite to any evidence to support its arguments concerning the purpose or intent of the amendments to CTCL's 2018 Articles of Association, including its claim that the amendments "were introduced only in the broader context of the Chinese government's reform of supervision and management of state-owned assets." *See* CTA Mar. 1, 2021 Reply at 50. CTA had also failed to provide evidence to support similar arguments that it made in its June 8, 2020 Response to the *Order to Show Cause*. *Institution Order*, 35 FCC Rcd at 15019, para. 23.

[242] *Institution Order*, 35 FCC Rcd at 15019, para. 23 (citing CTA June 8, 2020 Response, Exh. 15 at 6). In its June 8, 2020 Response, CTA argues that "[t]he purpose of the [Articles of Association] amendments was to further improve the corporate governance of [state-owned enterprises (SOEs)], standardize the relationship between party organizations and other corporate governance bodies (such as the board of directors) in corporate governance" and that "such [Articles of Association] Amendments have been recognized by certain investors, including foreign investors, as increasing the clarity and transparency of the role of Party organization in SOEs." CTA June 8, 2020 Response, Exh. 15 at 6.

[243] CTA Mar. 1, 2021 Reply at 50; *see also* CTA June 8, 2020 Response, Exh. 15 at 6.

[244] CTA Mar. 1, 2021 Reply at 50.

[245] *Id*.; CTA June 8, 2020 Response, Exh. 16 at 49.

[246] *See Institution Order*, 35 FCC Rcd at 15018-20, para. 23.

committees within all of these companies,"[247] and "[a]s part of these Party building activities, state-owned enterprises . . . are being pressured to amend their articles of association to ensure Party representation on their boards of directors . . . and to ensure that important company decisions are made in consultation with Party committees."[248] The national security and law enforcement concerns associated with the ability of the Chinese Communist Party to exercise influence and control over CTA, whether directly or through its parent entities, thus exist notwithstanding CTA's claim that its articles of incorporation and by-laws "contain no references to any foreign government, any of its agencies, or any foreign political party."[249]

59. Moreover, we find that the Chinese government has the ability to influence CTA through {[ ]}.[250] These 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.[251] The U.S. government has found that the Chinese government exerts influence over state-owned enterprises through the Chinese Communist Party. For example, USTR's 2018 Report on Findings of the Investigation into China's Acts, Policies, and Practices, states that "[t]he guiding principles for government ownership and control are set forth in the Constitution of the People's Republic

[247] Executive Branch Recommendation to Revoke and Terminate, Exh. 116 at EB-2568, U.S. Trade Representative, 2018 Report to Congress on China's WTO Compliance, at 13 (Feb. 2019) (2018 USTR Report to Congress on China's WTO Compliance); *id.* (stating, "both state-owned enterprises and private Chinese companies host internal Party committees capable of exercising government and Party influence over their corporate governance and business decisions. This arrangement is actually codified in Chinese law under Article 19 of the *Company Law*, which applies to both state-owned enterprises and private Chinese companies.").

[248] *Id.*, Exh. 116 at EB-2568, 2018 USTR Report to Congress on China's WTO Compliance; *id*. at 35 (citing *China Mobile USA Order*, 34 FCC Rcd at 3370, para. 18, n.60; Executive Branch Recommendation to Revoke and Terminate, Exh. 116 at EB-2568).

[249] CTA Mar. 1, 2021 Reply at 50; CTA June 8, 2020 Response, Exh. 16 at 49.

[250] *See supra* para. 51; *Institution Order*, 35 FCC Rcd at 15018-20, para. 23.

[251] Executive Branch Recommendation to Revoke and Terminate, 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); *id.*, Exh. 114 at EB-2384-2411, Revised Constitution. The Revised Constitution 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." *Id.*, Exh. 113 at EB-2381. The Executive Branch agencies state that "[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." Executive Branch Response at 13 (citing Executive Branch Recommendation to Revoke and Terminate, Exh. 8 at EB-371, 2019 Worldwide Threat Assessment by the Director of National Intelligence); *see also* Executive Branch Response at 12 ("[CTA's] public statements show that it is an active participant in the [Chinese] government's foreign policy, particularly with respect to the [Chinese] Belt and Road Initiative."); Executive Branch Recommendation to Revoke and Terminate, Exh. 60 at EB-1055, 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 the U.S. Trade Representative, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF (2018) (USTR Section 301 Report) ("in December 2017, NDRC [National Development and Reform Commission] and other [Chinese] government authorities jointly released a notice establishing behavioral norms for 'private enterprises' (*minying qiye*) investing abroad. This measure provides, for example, that private enterprises are to participate in the 'One Belt One Road' initiative, promote international industrial capacity and equipment manufacturing cooperation, act in the interest of the Chinese government's supply side structural reform agenda, and help 'protect China's sovereignty (*guojia zhuquan*), security (*guojia anquan*), and public interest (*shehui gonggong liyi*).'"). *See also* CTA Mar. 1, 2021 Reply at 54-58 ("These statements are exactly what could be expected from a pure commercial actor, and do not evidence any endorsement or support of the [Chinese] government's foreign policy or foreign policy objectives").

of China . . . and the [Chinese Communist Party] Constitution."[252] The report adds that, "[t]hrough the [Chinese Communist Party], the Chinese government exercises additional control over [state-owned enterprise] behavior."[253] Moreover, the Executive Branch agencies observe that, "[a]ccording to the Chinese government, the constitutional amendments were made to 'define the status and role of Party organizations in State-owned enterprises.'"[254] According 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."[255] Significantly, the Resolution on the Revised Constitution states that "the Party exercises overall leadership over all areas of endeavor in every part of the country,"[256] and "[Party members are obligated] to consciously observe the Party's political discipline and rules."[257] The record evidence detailing the scope of influence and control of the Chinese Communist Party, in light of CTCL's amended Articles of Association {[ ]} persuades us of the Chinese government's ability to influence and control CTA and its parent entities through Chinese Communist Party organizations, evidence that CTA has failed to refute.

60. We find that CTA and its parent entities are highly likely to be forced to cooperate with Chinese government requests without sufficient legal procedures subject to independent judicial oversight. This determination is based on the Chinese government's influence and control over CTA and its direct and indirect parent entities, combined with {[ ]} and the requirements of Chinese laws that have been enacted in recent years.[258] The combination of these

[252] Executive Branch Recommendation to Revoke and Terminate, Exh. 60 at EB-1063, USTR Section 301 Report (emphasis omitted); *see also id.*, Exh. 116 at EB-2566-2568, 2018 USTR Report to Congress on China's WTO Compliance (discussing that, "[t]o fulfill these [constitutional] mandates, the government and the Party direct and channel economic actors to meet the state's planning targets").

[253] *Id*., Exh. 60 at EB-1066, USTR Section 301 Report.

[254] *Id*. at 36 (citing *id.*, Exh. 113 at EB-2382, Resolution on the Revised Constitution).

[255] *Id*., Exh. 114 at EB-2404, Revised Constitution; *Institution Order*, 35 FCC Rcd at 15018-19, para. 23, n.80. Article 33 of the Revised Constitution directs that "[p]rimary-level Party organizations in state-owned or collective enterprises should focus their work on the operations of their enterprise." Executive Branch Recommendation to Revoke and Terminate, Exh. 114 at EB-2404.

[256] Executive Branch Recommendation to Revoke and Terminate, Exh. 113 at EB-2382, Resolution on the Revised Constitution (stating, "[t]he Congress holds that the leadership of the Communist Party of China is the most essential attribute of socialism with Chinese characteristics, and the greatest strength of this system; the Party exercises overall leadership over all areas of endeavor in every part of the country. The Congress agrees to add this major political principle to the Party Constitution, which will help heighten the Party consciousness of every Party member, and ensure unity of thinking, political solidarity and concerted action of the whole Party. It will also help enhance the Party's ability to innovate, power to unite, and energy to fight; ensure the Party always provides overall leadership and coordinates the efforts of all involved; and offer the fundamental political guarantee for all areas of work of the Party and the country."); *Institution Order*, 35 FCC Rcd at 15019, para. 23, n.81 (citing State-owned Assets Supervision and Administration Commission of the State Council, *What We Do*, http://en.sasac.gov.cn/2018/07/17/c_7 htm (updated July 17, 2018), and noting that "[t]he Party Committee of [the State-owned Assets Supervision and Administration Commission of the State Council] performs the responsibilities mandated by the Central Committee of the Chinese Communist Party").

[257] Executive Branch Recommendation to Revoke and Terminate, Exh. 113 at EB-2382, Resolution on the Revised Constitution.

[258] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 37-40.

laws—the 2017 Cybersecurity Law,[259] the 2018 Cybersecurity Regulation,[260] and the 2017 National Intelligence Law[261]—raises substantial and serious national security risks. First, we conclude that the 2017 Cybersecurity Law gives the Chinese government authority over the operations of CTA's parent entities.[262] CTA does not dispute this, but contends that the 2017 Cybersecurity Law "gives the Chinese government no authority over CTA's operations in the United States,"[263] and that the 2018 Cybersecurity Regulation "was formulated and promulgated according to the Cybersecurity Law and the Police Law of the People's Republic of China" and those laws "are applicable only within the territory of China."[264] We find, as indicated by the Executive Branch agencies, however, that the 2017 Cybersecurity Law "requires extensive cooperation by telecom and network operators" with the Chinese government.[265] For example, 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."[266] Additionally, Article 49 of the 2017 Cybersecurity Law states that "[n]etwork operators shall cooperate with cybersecurity and informatization departments and relevant

[259] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 38-40; *id*., Exh. 51 at EB-866, 2017 Cybersecurity Law.

[260] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 38-40 (citing *id.*, Exh. 54 at EB-903-905, EB-907, EB-909).

[261] *Institution Order*, 35 FCC Rcd at 15018, para. 22; Executive Branch Recommendation to Revoke and Terminate at 35 & n.123; *id*., Exh. 118 at EB-2735, 2017 National Intelligence Law.

[262] *Institution Order*, 35 FCC Rcd at 15020, para. 24; Executive Branch Recommendation to Revoke and Terminate at 38-39 ("According to the Parent Entity's interpretation of the 2017 Cybersecurity Law, the law sets forth a 'cybersecurity review' that government authorities could initiate that would focus on the 'controllability' of network products and services.") (citing *id.*, Exh. 4 at EB-86, CTCL Apr. 27. 2018 Form 20-F); *see also* Executive Branch Recommendation to Revoke and Terminate, Exh. 4 at EB-52 ("Substantially all of our assets are located in the [People's Republic of China] and substantially all of our revenues are derived from our operations in the [People's Republic of China]. Accordingly, our results of operations and prospects are subject, to a significant extent, to the economic, political and legal developments in the [People's Republic of China].").

[263] CTA June 8, 2020 Response, Exh. 16 at 56; *Institution Order*, 35 FCC Rcd at 15020, para. 24.

[264] CTA June 8, 2020 Response, Exh. 16 at 56; *Institution Order*, 35 FCC Rcd at 15020, para. 24.

[265] Executive Branch Recommendation to Revoke and Terminate at 38-39 (addressing Articles 35 and 49 of the 2017 Cybersecurity Law); *id.*, Exh. 51 at EB-876 and EB-880, 2017 Cybersecurity Law, Articles 35 and 49; *Institution Order*, 35 FCC Rcd at 15018, para. 22 & n.77; *see also* Executive Branch Recommendation to Revoke and Terminate, Exh. 51 at EB-869, 2017 Cybersecurity Law, Article 8 (stating, "[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."); *id.*, Exh. 4 at EB-86, CTCL Apr. 27. 2018 Form 20-F ("Telecom operators shall comply with the requirements under the Cybersecurity Law of the People's Republic of China in respect of network operating security and network information security.").

[266] Executive Branch Recommendation to Revoke and Terminate, Exh. 51 at EB-876, 2017 Cybersecurity Law; *see also id.* at 38-39; *id.*, Exh. 4 at EB-86, CTCL Apr. 27. 2018 Form 20-F. In its Form 20-F filed with the U.S Securities and Exchange Commission for the fiscal year ended December 31, 2017, CTCL stated, in addressing "Regulatory and Related Matters," that the 2017 Cybersecurity Law "require[s] procurement of network products and services by operators in key industries or of critical information infrastructure facilities that may have national security concerns to go through a cybersecurity review. Relevant government authorities responsible for the protection of critical information infrastructure facilities will decide on whether such procurement would threat national security pursuant to the review. The security review of telecommunications industry would be organized and conducted by the [Ministry of Industry and Information Technology]. The security review may be initiated by the enterprises or by the relevant government authorities. The security review would focus on the security and controllability of network products and services." *Id.*

departments in conducting implementation of supervision and inspections in accordance with the law."[267] Further, the 2018 Cybersecurity Regulation "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 or, for remote inspections, the use of certain cybersecurity service agencies.[268]

61. We also believe that CTA is vulnerable to Chinese government requests based on the requirements of the 2017 Cybersecurity Law and the 2018 Cybersecurity Regulation, and that the 2018 U.S. Records Security Agreement between CTA and its direct parent entity, CTCL, exemplifies such vulnerability. As an initial matter, {[

]}[269] CTA provided the 2018 U.S. Records Security Agreement to the Executive Branch agencies on December 6, 2018, {[

]}[270] In its March 1, 2021 Reply, CTA disputes the significance of this Agreement, contending that "instead of providing any evidence showing that CTA is vulnerable to 'foreign government' requests, the only example provided in support of the Executive Branch's allegation is based on a (mis)interpretation of [the Agreement]."[271] CTA cites to its June 8, 2020 Response where it argues, "CTA entered into an arms-length Records Security Agreement with its parent company expressly for, among other things, the purpose of ensuring compliance with the LOA" and "the Recommendation seems to suggest the irrational inference that by entering into a commercial agreement, CTA demonstrated its vulnerability to be directed by and comply with Chinese Government requests."[272]

62. Contrary to CTA's claims, we find that the 2018 U.S. Records Security Agreement is an example of how {[

]}[274] Significantly, upon further inquiry by the Executive Branch agencies, CTA admitted that its U.S. records are available to its non-U.S. affiliates

[267] *Id.*, Exh. 51 at EB-880, 2017 Cybersecurity Law; *see also id.* at 38-39.

[268] *Id.* at 39-40 (citing *id.*, Exh. 54 at EB-904, EB-905, EB-907, EB-909).

[269] *Id*., Business Confidential Exh. 36 at EB-589-590, EB-630, December 6, 2018 Letter with Attachments.

[270] CTA June 8, 2020 Response, Exh. 16 at 22 & n.40 (citing "Recommendation Exhibit 36 at EB-590 (introducing the U.S. Records Security Agreement)" and "Recommendation Exhibit 36 at EB-624"); *id.*, Exh. 16 at 27-28; Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586-587, November 26, 2018 Email; *id.*, Business Confidential Exh. 36 at EB-589-590, December 6, 2018 Letter with Attachments.

[271] CTA Mar. 1, 2021 Reply at 32; *see also* CTA June 8, 2020 Response, Exh. 16 at 52 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621, EB-625-26).

[272] CTA June 8, 2020 Response, Exh. 16 at 52.

[273] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621, December 6, 2018 Letter with Attachments.

[274] *See id.*, Business Confidential Exh. 36 at EB-621-630, EB-634, EB-636, December 6, 2018 Letter with Attachments; *id.*, Business Confidential Exh. 103 at EB-2111-13, Apr. 4, 2019 Letter from Morgan Lewis to DOJ National Security Division (April 4, 2019 Letter); *see also infra* Section III.B.3. ({[
]}).

abroad, {[ ]}[275] This is particularly concerning given the Executive Branch agencies' observation that "[b]oth the 2017 Cybersecurity Law and 2018 [Cybersecurity Regulation] provide little, if any, detail about the available legal procedures or judicial oversight to challenge any Chinese government requests."[276]

63. At the outset, CTA offers no additional evidence for its assertion that the Commission's concerns "result[] from its misunderstanding of the Chinese laws" and fails to explain this argument with particularity.[277] Additionally, the 2017 National Intelligence Law raises concerns about CTA's vulnerability to exploitation, influence, and control by the Chinese government. In fact, 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."[278] The former U.S. National Security Advisor has also noted that under Article 7 of China's National Intelligence Law, "all Chinese companies must collaborate in gathering intelligence."[279] Additionally, the Office of the Secretary of Defense stated in its 2019 report on Military and Security Developments Involving the People's Republic of China 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."[280] CTA did not address this evidence in the record, and we find nothing in the record to refute these concerns. CTA states instead that it "is not in any position to express an opinion about the Executive Branch's position on alleged policies of the Chinese

---

[275] *See* CTA June 8, 2020 Response, Exh. 16 at 21-22; Executive Branch Recommendation to Revoke and Terminate at 19 (citing *id.*, Business Confidential Exh. 103 at EB-2111-12); *see infra* Section III.B.3. {[ ]} Executive Branch Recommendation to Revoke and Terminate at 20 (citing *id*., Business Confidential Exh. 103 at EB-2113); *id*., Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments ({[ ]} "was implemented voluntarily by CTA in an effort to assure continued compliance with the LOA." CTA June 8, 2020 Response, Exh. 16 at 38. {]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112-13, April 4, 2019 Letter; *id.*, Business Confidential Exh. 36 at EB-624; *see infra* para. 104 ({[ ]}).

[276] Executive Branch Recommendation to Revoke and Terminate at 40.

[277] CTA Mar. 1, 2021 Reply at 33 & n.121 (citing *Institution Order*, 35 FCC Rcd at 15020, para. 24; CTA June 8, 2020 Response, Exh. 16 at 4-5, 47-57).

[278] Executive Branch Recommendation to Revoke and Terminate, Exh. 118 at EB-2738, 2017 National Intelligence Law.

[279] *See 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 (*What China Wants*); H.R. McMaster, *How China Sees the World: And How We Should See China* (May 2020), https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/); *see also* Executive Branch Recommendation to Revoke and Terminate, Exh. 120, EB-2747-50, *Beijing's New National Intelligence Law*.

[280] Executive Branch Recommendation to Revoke and Terminate 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)).

government."[281] However, we find based on the record that CTA is subject to national security risks because of these identified laws and its relationship with its direct and indirect parent entities, and in light of the 2018 U.S. Records Security Agreement, and thus is subject to exploitation, influence, and control by the Chinese government.

64. In fact, as discussed below, the national security and law enforcement risks associated with these laws, combined with the 2018 U.S. Records Security Agreement, show that the risks "are no longer theoretical."[282] CTA disclosed in an April 4, 2019 Letter to the Executive Branch agencies that "'[b]eginning in May 2013, when the {[ ]} was implemented, U.S. records were available to CTA's non-US affiliates abroad.'"[283] {[

]}[285] The Executive Branch agencies also state their concern given that the 2018 U.S. Records Security Agreement indicates that {[

]}[286] Contrary to CTA's claims, the overall risks we identify here are not overstated[287] and our interpretation of Chinese laws is not taken out of context.[288] Moreover, we find no evidence in the record {[ ]}[289] will not be subject to any request or directive from the Chinese government, or that CTA would be able to challenge or act independently of any such request or directive related to the Chinese government. {[

[281] CTA Mar. 1, 2021 Reply at 43; *see also* CTA June 8, 2020 Response, Exh. 16 at 46.

[282] *Institution Order*, 35 FCC Rcd at 15020, para. 25; *see also infra* Section III.B.3.

[283] CTA June 8, 2020 Response, Exh. 16 at 28 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111). *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111, April 4, 2019 Letter; *id.* at 19; *see infra* para. 104 ({[ ]}). *See also Institution Order*, 35 FCC Rcd at 15029, para. 38.

[284] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112, April 4, 2019 Letter; *id.*, Business Confidential Exh. 96 at EB-2000-03, March 21, 2019 Letter; *id.*, Business Confidential Exh. 102 at EB-2103-06, March 21, 2019 Letter; *id.* at 19; *see infra* para. 104 ({[ ]}).

[285] Executive Branch Recommendation to Revoke and Terminate at 40; *Institution Order*, 35 FCC Rcd at 15020, para. 25, n.92.

[286] Executive Branch Recommendation to Revoke and Terminate at 37-38 (citing *id*., Business Confidential Exh. 36 at EB-621); *Institution Order*, 35 FCC Rcd at 15020-21, para. 25.

[287] CTA June 8, 2020 Response, Exh. 16 at 29. CTA contends that "Team Telecom vastly overstates the risks associated with CTA's U.S. Records given the actual content and locations of those records," and "the types of information that CTA shares with its non-U.S. affiliates are substantially the same types of information that ***any*** U.S. carrier, regardless of its ownership, likely would have to provide to a Chinese carrier if it wants to deliver international services between the two countries." *Id.*

[288] *Id*., Exh. 16 at 55.

[289] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111-13, 6April 4, 2019 Letter; *id.*, Business Confidential Exh. 36 at EB-621-627, 634, December 6, 2018 Letter with Attachments.

]}[290] The record evidence regarding CTA's corporate governance and the officers, directors, and senior management officials of CTA and its parent entities, combined with Chinese laws and the terms of CTA's 2018 U.S. Records Security Agreement, raises significant and substantial national security and law enforcement concerns that require revocation of CTA's domestic and international section 214 authority.

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

65. Given the changed national security environment since the Commission authorized CTA to provide telecommunications services in the United States and based on our review of the full record in this proceeding, we conclude there are significant national security and law enforcement risks associated with CTA's retention of its section 214 authority that pose a clear and imminent threat to the security of the United States. As explained below, CTA's operations in the United States pursuant to its domestic and international section 214 authority, combined with those operations not authorized under section 214 authority, provide CTA with access to U.S. telecommunications infrastructure and sensitive U.S. customer information. CTA's service offerings in the United States make it potentially more attractive to U.S. customers and to U.S. industries[291] seeking telecommunications services than if it were located outside of the United States, thus enhancing CTA's access to such U.S.-based infrastructure and information. As discussed below, this access presents CTA, 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 the national security and law enforcement interests of the United States. Because the Chinese government has influence and control over CTA, as discussed above, the record raises serious and unacceptable concerns that the Chinese government can, for example, influence or direct CTA to act on any of these opportunities presented by its access to U.S. telecommunications infrastructure and U.S. customer information.[292] Despite being provided several opportunities to address these national security

[290] {[

]}

See CTA June 8, 2020 Response, Exh. 16 at 38, n.74 ("Even if CTA did not implement this private, inter-company agreement strictly according to its terms, this would not demonstrate any violation of an LOA commitment or of any Commission rule . . . .").

[291] *See, e.g.*, Executive Branch Recommendation to Revoke and Terminate at 42 (stating, "[CTA] intentionally markets its services as secure to customers in industries highly vulnerable to economic espionage, such as the financial, logistics, retail, media, energy, and healthcare industries") (citing *id.*, Exh. 42 at EB-699, Screenshot, Financial, China Telecom Americas, https://www.ctamericas.com/industry-solutions/financial (accessed Feb. 15, 2019)); China Telecom (Americas) Corporation, https://www.ctamericas.com/ (displaying advertised "Products" and "Solutions"). *See also* CTA June 8, 2020 Response, Exh. 16 at 44 ("CTA does not seek out customers in particular industries; rather, CTA seeks out customers in any industry who have a particular need for communications with China").

[292] *See Institution Order*, 35 FCC Rcd at 15016-17, 15023-29, paras. 20-21, 29-36; Executive Branch Recommendation to Revoke and Terminate at 2-7 (discussing that "[t]he national security environment has changed significantly since 2007").

and law enforcement risks, CTA failed to persuasively dispute or explain how these risks can be ameliorated.[293] Indeed, CTA did not address with particularity or otherwise respond to the national security and law enforcement concerns that were raised by the Commission on these matters in the *Institution Order*.[294] Accordingly, we conclude that CTA's retention of section 214 authority presents national security and law enforcement risks that warrant revocation of its section 214 authority.

66. CTA has blanket domestic section 214 authority and holds two international section 214 authorizations. CTA states that it provides telecommunications and non-telecommunications services in the United States and that "[s]ome telecommunications capabilities are provided as common carrier services pursuant to domestic and/or international section 214 authorizations, while some are provided on a private carrier basis."[295] CTA identifies nine services that it describes as "Communications and Internet Services," but does not specify which of these services require section 214 authority.[296] Of these nine services, based on CTA's filings, CTA appears to currently offer the following services pursuant to its section 214 authority: MVNO, IPLC, IEPL, and MLPS VPN services.[297] CTA is authorized to, at any time, provide any other domestic service under blanket section 214 authority,[298] and to provide "international basic switched, private line, data, television and business services" under section 214 of the Act and its implementing rules.[299] This authority allows a carrier to continue to extend its existing network, install new equipment or upgrade existing equipment on its network, or request additional interconnections with the networks of other U.S. common carriers[300]—all without seeking further Commission approvals.[301]

67. Circumstances have since changed dramatically since the Commission authorized CTA to provide telecommunications services in the United States. Additionally, the Executive Branch agencies recognize that the national security environment has changed significantly since 2007 when CTA entered into its LOA with the Executive Branch agencies.[302] As the Executive Branch agencies explain, the top

[293] *See* CTA June 8, 2020 Response, Exh. 16 at 3-4, 5, 57-63; CTA March 1, 2021 Reply at 33.

[294] CTA March 1, Reply at 33 (stating generally, "CTA disputes that its U.S. operations provide opportunities for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic"); *see Institution Order*, 35 FCC Rcd at 15023-29, paras. 29-36.

[295] CTA June 8, 2020 Response, Exh. 6 at 1; *see also* China Telecom (Americas) Corporation, https://www.ctamericas.com/ (displaying advertised "Products").

[296] *See* CTA June 8, 2020 Response, Exh. 6 at 1-6.

[297] *Id*.

[298] 47 CFR § 63.01; *see supra* para. 8.

[299] 47 U.S.C. § 214; 47 CFR §§ 63.22(d), 63.23(c), 63.18(e)(1)-(2); *see supra* note 19.

[300] 47 U.S.C. § 214; 47 CFR § 63.02(a); *see also China Mobile USA Order*, 34 FCC Rcd at 3377, para. 33, n.98 (stating that China Mobile International (USA) Inc. (China Mobile USA) would be able to request interconnection with the networks of other U.S. common carriers).

[301] 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).

[302] *See Institution Order*, 35 FCC Rcd at 15011-12, 15023-24, paras. 9, 30; *see also* Executive Branch Recommendation to Revoke and Terminate at 2-7.

concern of the U.S. Intelligence Community in 2007 was terrorism, "with the countries of highest concern being Iraq, Afghanistan and Pakistan."[303] The Executive Branch agencies note that, in the 2019 Worldwide Threat Assessment of the Office of the Director for National Intelligence (ODNI), "China is the first country identified by name for its persistent economic espionage and growing threat to core military and critical infrastructure systems."[304] Recently, 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."[305] 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."[306] 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.[307] For instance, the Executive Branch agencies indicate that DOJ has announced multiple indictments of Chinese state actors targeting the U.S. private sector.[308] According to the Executive Branch agencies, these escalated warnings about the threats

[303] Executive Branch Recommendation to Revoke and Terminate at 2 (citing *id.*, Exh. 7 at EB-335, *Annual Threat Assessment Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 3 (2007) (unclassified statement of John D. Negroponte, Director of National Intelligence)); *id.*, Exh. 7 at EB-334 ("Terrorist threats to the Homeland, to our national security interests, and to our allies remain the pre-eminent challenge to the Intelligence Community, operationally and analytically."); *see also Institution Order*, 35 FCC Rcd at 15023, para 30, n.114. The Executive Branch agencies note that "the Office of the Director of National Intelligence (ODNI) did not mention the word 'cyber' in its annual briefing to Congress on global threats." Executive Branch Agencies Recommendation to Revoke and Terminate at 2 (citing *id.*, Exh. 7 at EB-335).

[304] *Executive Branch Recommendation to Revoke and Terminat*e at 2 (citing *id.*, Exh. 8 at EB-351); *see also Institution Order*, 35 FCC Rcd at 15024, para 30. Additionally, ODNI's National Counterintelligence and Security Center warned in July 2018 that "the Chinese government seeks to enhance its collection of U.S. technology by enlisting the support of a broad range of actors spread throughout its government and industrial base." Executive Branch Recommendation to Revoke and Terminate, Exh. 82 at EB-1910, Foreign Economic Espionage in Cyberspace, National Counterintelligence and Security Center at 5 (July 26, 2018), https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf.

[305] 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.

[306] *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.*

[307] *See Institution Order*, 35 FCC Rcd at 15011-12, 15023-24, paras. 9, 30; Executive Branch Recommendation to Revoke and Terminate at 2-7; Executive Branch Response at 10; *see, e.g.*, Executive Branch Recommendation to Revoke and Terminate at 6 (noting, "in its November 2018 Update to its Section 301 findings, the U.S. Trade Representative raised alarms that incidents of Chinese cyber thefts were rapidly accelerating"); *id.*, Exh. 90 at EB-1971, Christopher Wray, Keeping our Financial Systems Secure: a Whole-of-Society Approach, Ninth Annual Financial Crimes and Cybersecurity Symposium, https://go.usa.gov/x6e4t (Nov. 1, 2018) ("No country poses a broader, more severe intelligence collection threat than China. [] Nearly every FBI field office currently has economic espionage cases that lead back to China."); *id.*, Exh. 59 at EB-973, China's Non-traditional Espionage Against the United States: The Threat and Potential Policy Responses at 1, Hearing Before the S. Comm. on the Judiciary, 115th Cong. (Dec. 12, 2018) (statement of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security) ("Nation-state threat actors such as China . . . have used cyber intrusions to steal private sector proprietary information and sabotage military and critical infrastructure. [] China will continue to use cyber espionage and bolster cyber attack capabilities to support its national security priorities.").

[308] Executive Branch Recommendation to Revoke and Terminate at 4. The Executive Branch agencies state that "[s]ince the Economic Espionage Act was passed in 1996, about 80 percent of DOJ's economic espionage cases (involving trade secret theft where the defendant knew or intended that his theft would benefit a foreign government, instrumentality, or agent) have involved China, and most trade secret theft cases have had some nexus to China." *Id.* *See also* DOJ, Information about the Department of Justice's China Initiative and a Compilation of China-Related

(continued….)

posed by Chinese government-sponsored cyber actors in the current national security environment "are not limited to direct acts by the Chinese government, but also include the Chinese government's potential use of Chinese information technology firms as routine and systemic espionage platforms against the United States."[309]

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

68. Based on the totality of the evidence in the record, we find that the variety of services offered by CTA pursuant to its section 214 authority, as well as those not authorized pursuant to section 214 authority, provide CTA with access to U.S. telecommunications infrastructure and U.S. customer records. This access presents CTA, 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.[310] In particular, the suite of services that CTA provides pursuant to its section 214 authority, such as MVNO, IPLC, IEPL, and MPLS VPN services, together with its ability to combine some of these and other non-section 214 services as a managed services provider (MSP),[311] makes CTA more attractive as a service provider to U.S. customers than if it did not offer such services. This in turn increases the prospective U.S. customer base for CTA's section 214 services and other services that are operated directly or indirectly through Internet Exchange (IX) points[312] and private peering points.[313] The full suite of services offered by CTA, including services pursuant to section 214 authority and other services, facilitated by CTA's physical presence in the United States, creates a significant opportunity for CTA to conduct activities that are harmful to the national security and law enforcement interests of the United States.

69. As discussed below, the opportunities for harmful conduct associated with CTA's ability, as a service provider, to carry U.S. communications traffic present risks of unauthorized access to U.S. customer data and/or metadata.[314] The record evidence shows that CTA's U.S. records are already

(Continued from previous page)
Prosecutions Since 2018, https://www.justice.gov/nsd/information-about-department-justice-s-china-initiative-and-compilation-china-related (last updated June 14, 2021).

[309] Executive Branch Recommendation to Revoke and Terminate at 41 (citing *id.*, Exh. 8 at EB-351); *Institution Order*, 35 FCC Rcd at 15024, para. 31, n.116.

[310] Executive Branch Recommendation to Revoke and Terminate at 42-43.

[311] CTA June 8, 2020 Response, Exh. 6 at 1-5, 8; *see also* China Telecom (Americas) Corporation, *Data Networking*, https://www.ctamericas.com/products-services/data-networking/ (last visited Sept. 20, 2021); *see also, e.g.*, China Telecom (Americas) Corporation, *Product Overview* at 2 (2016), https://www.ctamericas.com.cn/wp-content/uploads/2016/12/Product-Overview.pdf (*CTA Product Overview*) (presenting overview of CTA and products, including incorporation of CTA's MSP service, Netcare, with MPLS VPN service).

[312] *See* Cloudflare, *What is an Internet Exchange Point? | How do IXPs work?*, https://www.cloudflare.com/learning/cdn/glossary/internet-exchange-point-ixp/ (last visited Oct. 2, 2021) ("An Internet exchange point (IXP) is a physical location through which Internet infrastructure companies such as Internet Service Providers (ISPs) and CDNs [content delivery network] connect with each other").

[313] *See* Telehouse, *Internet Exchange Services*, https://www.telehouse.com/solutions/connectivity/peering/ (discussing difference between private and public peering); PeeringDB, *CTANET*, https://www.peeringdb.com/net/18639 (last visited Sept. 22, 2021) (*PeeringDB CTANET*) (indicating that "CTA" is available for private peering at several facilities).

[314] 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#:~:text=%2F%CB%88met%C9%99d%C3%A6t%C9%99%2F,you%20understand%20or%20use%20it (last visited Oct. 2, 2021) (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." (continued….)

available to its non-U.S. affiliates abroad, {[

]}[316] The Executive Branch agencies also note, {[

]}[317] We discuss below how CTA's provision of certain services pursuant to section 214 authority, including MVNO service, provide significant opportunity for unauthorized access to U.S. records and other customer information.

70. In addition to this practice involving access to its U.S. records, CTA further has the ability and opportunity to engage in, as well as facilitate for its parent entities and affiliates, unauthorized access to U.S. customer data and/or metadata through traffic path diversions or intentional misrouting. As an initial matter, CTA has the ability to cause 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 CTA may have in place with its ultimate parent entity CT, in the course of operating on CT's network.[318] However, 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, but more important and relevant to our assessment here, is that path diversions 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. Significantly, CTA, 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[319] of traffic by CTA, through a process described below.

(Continued from previous page)
See ComputerWorld, *Data retention: Law enforcement accessed 'metadata' more than 296k times in FY18* (July 23, 2019), https://www.computerworld.com/article/3472422/data-retention-law-enforcement-accessed-metadata-more-than-296k-times-in-fy18.html.

[315] *See* CTA June 8, 2020, Exh. 16 at 21-22; Executive Branch Recommendation to Revoke and Terminate at 19 (citing *id.*, Business Confidential Exh. 103 at EB-2111-12); *id.*, Business Confidential Exh. 36 at EB-621-634, December 6, 2018 Letter with Attachments; *see supra* para. 64.

[316] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621, December 6, 2018 Letter with Attachments. {[

]} *Id.*, Business Confidential Exh. 36 at EB-623.

[317] *Id*. at 40; *Institution Order*, 35 FCC Rcd at 15020, para. 25, n.92.

[318] *See infra* note 384 (discussing peering policies).

[319] Misrouting is the configuration of routing policies, or advertising of false routes, to ensure that traffic is forwarded through locations from which bad actors can monitor and/or manipulate data using sub-optimal routes (i.e., routes that are not the shortest path, nor reflect a least cost path, between the origination and destination). *See, e.g.*, Executive Branch Recommendation to Revoke and Terminate at 44-48; *Institution Order*, 35 FCC Rcd at 15024-25, para. 31.

71. While we recognize that any service provider has the opportunity to engage in traffic path diversions or intentional misrouting, other such providers are not identified like CTA as posing a national security and law enforcement risk.[320] CTA's network operates in conjunction with CT's network, and thus can utilize CT's infrastructure as part of the normal network operations associated with CTA's services.[321] Indeed, CTA describes its ability to leverage CT's network and infrastructure as an advantage in its company promotions.[322] Further, CTA is ultimately owned by the Chinese government and therefore subject to exploitation, influence, and control by the Chinese government. In light of the Chinese government's control over CTA and the numerous opportunities for CTA and its indirect parent company CT to access, monitor, store, disrupt and/or misroute U.S. communications in ways that are not authorized and that can facilitate espionage and other harmful activities, the overwhelming evidence presents serious and significant threats to the national security and law enforcement interests of the United States. These include threats to the security of the U.S. telecommunications infrastructure and the information that is carried on this infrastructure by the individuals and companies that use CTA's services.

(i) MVNO

72. We find that there are significant national security and law enforcement risks associated with CTA's retention of its section 214 authority to provide MVNO services, as described below, and we therefore reject CTA's request to retain its MVNO service based on "the lack of any potential harm from continuing service."[323] As an MVNO, CTA has the opportunity to collect a significant amount of customer information, including U.S. customers' personally identifiable information (PII), through call detail records (CDRs), provisioning and management of SIM cards, and metadata pertaining to customer communications, with or without the authorization of its customers. CTA, like all telecommunications carriers with access to this sensitive PII,[324] has a statutory responsibility to ensure the protection of

[320] *Institution Order*, 35 FCC Rcd at 15023-29, paras. 29-36.

[321] *See* CTA June 8, 2020 Response, Exh. 6 at 3-4, 8 (explaining that CTA provides IPLC, IEPL, MPLS VPN, and other services, using CT's network(s)); *see also id.*, Exh. 16 at 50 (stating that "CTCL," CTA's direct parent, "operates a global network, ChinaNet (AS 4134), which is a Tier 1 network and has many customers operating smaller networks who purchase transit service from it" and "CTA maintains POPs in the United States that provide access to this network for U.S. transit customers and peering partners"). CTA's webpage titled "Company Overview," states, in relation to CT, that "China Telecom Americas is the largest subsidiary of China Telecom Corporation, one of the world's leading providers of integrated communications and information technology services to enterprises in over 110 countries around the globe." *See* China Telecom (Americas) Corporation, *Company Overview—About Us*, https://www.ctamericas.com/company/company-overview/ (last visited Sept. 21, 2021). The webpage refers to "China Telecom" as "the largest operating broadband operator in the world with more than 135 million subscribers, and the world's largest CDMA mobile operator boasting more than 227 million subscribers," and states that China Telecom "[o]wns and operates three Tier 1 global networks" which include ChinaNet (AS 4134), CN2 (AS 4809) and CTG Net (AS 36778). *Id.* The webpage also displays a subheading, "China Telecom Corporation" where it refers to "China Telecom" in relation to CT. *Id.* In addition, CTA's webpage titled "Global Network" states that "China Telecom Americas delivers a comprehensive range of high quality telecommunications services to customers around the world," referring to "our Tier-1 global network" and "our ChinaNet network." China Telecom (Americas) Corporation, *Global Network*, https://www.ctamericas.com/company/global-network/ (last visited Sept. 21, 2021) (*CTA Global Network*).

[322] *See, e.g.*, China Telecom (Americas) Corporation, International Ethernet Private Line Service, https://www.ctamericas.com/wp-content/uploads/2018/10/IEPL.pdf (last visited Sept. 7, 2021).

[323] CTA Mar. 1, 2021 Reply at 62.

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

proprietary information about customers, including customer proprietary network information (CPNI).[325] Moreover, as a condition of its international section 214 authorizations, CTA was required but, as discussed below, failed to take "all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records . . . ."[326]

73. CTA explains that it "acts as an MVNO in the U.S. under the 'CTExcel' brand name, which CTA markets primarily to Chinese language users in the United States."[327] CTA resells service that is provided over the network of a Mobile Network Operator (MNO), through an arrangement with {[ ]}[328] CTA further explains that it "offers its resold mobile services through an MVNO aggregator," which is responsible for maintaining the direct commercial relationship with the underlying U.S. MNO and interconnecting to the carrier's business support systems.[329] The U.S. MNO then terminates all U.S. domestic calls and routes international calls to another U.S. carrier for international transport service to Hong Kong, for subsequent routing to the final destination.[330] The exact set of information collected by an MNO and disseminated to an MVNO and its aggregator(s) may vary, but information collected by an MNO generally will include sensitive information such as the calling number, called number, call duration, and location of cell tower.[331]

74. We find unpersuasive CTA's argument that, with respect to its resold mobile service, "the theoretical risk of any sensitive information falling into the hands of the Chinese government from within the U.S. is practically zero."[332] CTA has acknowledged in the record that it has direct access to sensitive U.S. customer information[333] in CDRs.[334] The need to protect each CDR has long been

[325] 47 U.S.C. § 222 ("Privacy of customer information"); *id.* § 222(a) ("Every telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier."); *see 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 (2007) *(CPNI Order*) (adopting rules to ensure that CPNI is adequately protected from unauthorized access, use, or disclosure).

[326] *See infra* para. 120.

[327] CTA June 8, 2020 Response, Exh. 16 at 34.

[328] *Id*., Exh. 16 at 34-35.

[329] CTA Mar. 1, 2021 Reply at 61; CTA June 8, 2020 Response, Exh. 16 at 34-35.

[330] CTA Mar. 1, 2021 Reply at 61; CTA June 8, 2020 Response, Exh. 16 at 34-35.

[331] *See, e.g.*, PATC Tech Digital Forensics, Cellular Records Review and Analysis Part 4: T-Mobile, at 5, http://nebula.wsimg.com/fe53805000f63a9e3d12e379df2fdcc2?AccessKeyId=5A68D373C291B31859BF&disposition=0&alloworigin=1 (last visited Oct. 2, 2021); *see also* 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.

[332] CTA Mar. 1, 2021, Reply at 61-62.

[333] "CDR" is a term of art and was initially attributed to circuit switched voice traffic. It 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*). *See also ACLU v. Clapper*, 785 F.3d 787, 793 (2nd Cir. 2015) (*ACLU v. Clapper*) (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 "call detail records"); Alliance for Telecommunications Industry Solutions (ATIS), *call detail recording*, ATIS Telecom Glossary,

(continued….)

recognized.[335] Even without revealing the content of communications, CDRs can reveal significant information.[336] 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,[337] including Africa, Asia, Europe, and the Middle East.[338] While service providers understandably focus their cybersecurity efforts on the need to protect their customers' CDRs from such hacking incidents,[339] 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 CTA, has direct access to CDRs, which facilitates opportunity to access and misuse such information.

75. Additionally, CTA's provisioning and management of SIM cards through its MVNO service provides CTA the opportunity to access and misuse its customers' information with relatively minimal effort and low risk of detection by customers. CTA offers SIM cards, a common business practice in the market for resold mobile services. Specifically, CTA offers a dual SIM product.[340] CTA

(Continued from previous page)
https://glossary.atis.org/glossary/call-detail-recording-cdr/?search=call%20detail%20recording&page_number=&sort=ASC (last visited Oct. 1, 2021); 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service aspects; Charging and Billing (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 "Charging" and "Billing"). The current 3GPP specifications use the term "Charging Data Record." *3GPP – Charging Data Record* at 23 (defining "Charging Data Record").

[334] CTA June 8, 2020 Response, Exh. 16 at 34-35. CTA describes its MVNO operations as follows: "CTA resells service over the T-Mobile network through an arrangement with {[ ]} interconnects to {[ ]} to provision mobile services on {[ ]} for a CTA customer. CTA collects basic billing information from subscribers, such as name, address, phone type, and credit card information, since consumers pay via credit card. CTA then provides to {[ ]} the information it needs to establish service. CTA's copy of the information provided to {[ ]} is held in the cloud on Amazon Web Services. {[ ]} *provides call detail records to CTA* for billing process and support, all of which are also maintained by CTA on Amazon Web Services. CTA's non-U.S. affiliates have no access to this information." *Id.* (emphasis added). *See also 3GPP – Charging and Billing* at 5; *3GPP – Charging Data Record* at 23.

[335] 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* Florin Vancea et al., *Secure Data Retention of Call Detail Records* (Int. J. of Computers, Communications, & Control: Vol. V, No. 5, at 961-963) (2010), https://www.researchgate net/publication/228991607_Secure_Data_Retention_of_Call_Detail_Records (*Secure Data Retention of Call Detail Records*).

[336] *See ACLU v. Clapper*, 785 F.3d at 794 (reviewing argument by appellants and amici about "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 also* 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).

[337] Whittaker; *see also* 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).

[338] *See* Porter.

[339] *See Secure Data Retention of Call Detail Records*.

[340] *See* CTA June 8, 2020 Response, Exh. 16 at 35-36; *id*, Exh. 6 at 5.

states that its MVNO service, CTExcel, offers "dual U.S. and Chinese telephone numbers on their phone as a service feature, allowing the user to have calls forwarded between their U.S. and China cell phone numbers."[341] Moreover, CTA explains that "[w]hen a customer purchases both U.S. and China phone numbers linked to a single SIM card, Chinese government regulations require that CTA's Chinese affiliate (not CTA itself) obtain PII about the user to comply with Chinese law to provide mobile service in China."[342] Importantly, CTA, like all service providers that have access to SIM cards, also has access to private and sensitive customer information (e.g., phone book entries including email addresses).[343] In addition, through the use of Over-The-Air (OTA) provisioning, providers of SIM cards, including CTA as an MVNO and other MVNOs and MNOs, can provision, update, and even change the content of SIM cards.[344]

76. CTA's MVNO service offering provides CTA with access to sensitive customer information through CDRs and SIM cards. Moreover, the sensitivity of the information can be greatly enhanced and pose even greater risks when it is combined with other information that CTA can access from network communications and data, as well as network metadata.[345] The information to which CTA has access includes customer PII, including billing information such as name, address, payment details such as credit card numbers, and other data.[346] As the *Institution Order* stated, "collection and maintenance of records pertaining to the provision and billing for services do not comprise the sole means by which [CTA], or any other service provider, can collect records about its customers."[347] CTA, like any service provider, could also "analyze application content or metadata derived from packets transiting a device or infrastructure that is managed by the service provider."[348] Further, "any monitoring of connectivity and transmission can provide substantial, and highly valuable, information that could potentially be used for espionage."[349]

77. CTA claims that "the records [it] collects and maintains about its customers are those necessary to provision and bill for services and are substantially similar to the records that *any* U.S. carrier would have to share with Chinese carriers to enable service between U.S. and China."[350] As stated

[341] *Id*., Exh. 6 at 5. CTA explains that "[i]ndividual consumers purchase CTA's CTExcel SIM card and obtain service on a monthly basis for the plan of their choice." *Id*.

[342] *Id*., Exh. 16 at 35. CTA states that "[i]f a user requests a dual phone number, they must supply the following to that [CTA] affiliate directly:" (1) legal name of the user; (2) Chinese photo ID with the expiration date and the place of issue, a foreign passport with a valid visa to China, or a "China Pass" document issued to residents of Hong Kong, Macau, and Taiwan; (3) a photo of the applicant holding their own ID; and (4) a Chinese number bill (if the applicant applies to have their existing Chinese number as the dual number). *Id*.

[343] 3rd Generation Partnership Project (3GPP), 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Characteristics of the Universal Subscriber Identity Module (USIM) Application (Release 17) (3GPP TS 31.102 V17.2.0) (June 2021), at 146-47, https://www.3gpp.org/ftp/Specs/archive/31_series/31.102/31102-h20.zip.

[344] *See, e.g.*, EMnify, *What is Over-the-Air? OTA Provisioning Explained* (Dec. 22, 2020), https://www.emnify.com/en/resources/over-the-air (stating, "OTA provisioning refers more specifically to the process of updating or modifying something wirelessly" and "[t]hese OTA technologies allow changing the content of the SIM card or even changing a full operator profile").

[345] *See supra* note 314 (discussing metadata).

[346] *See TerraCom NAL*, 29 FCC Rcd at 13331, para. 17.

[347] *Institution Order*, 35 FCC Rcd at 15025, para. 33.

[348] *Id*.

[349] *Id*. at 15027, para. 35.

[350] CTA June 8, 2020 Response, Exh. 16 at 58; *id*., Exh. 16 at 29-30 (stating that CTA "collects and maintains only limited customer information as U.S. Records"). *But see supra* para. 75 (discussing collection of PII of MVNO (continued….)

in the *Institution Order*, "[w]hile it may be true that the records CTA collects are similar to those that U.S. carriers would need to share with Chinese carriers to enable international services, such U.S. carriers do not have a similar relationship with their parent company controlled by a foreign government that has imposed legal and corporate restrictions of the kind under which [CTA] is now required to operate."[351] Like similarly situated service providers, CTA is able at any time to misuse customer data to engage in malicious behavior, such as the theft of trade secrets and other confidential customer or business information from the data and communications which its customers, or those interacting with CTA's customers, entrust to CTA. Unlike many other service providers, however, CTA is indirectly owned and controlled by the Chinese government, which has imposed legal and corporate restrictions under which CTA and its parent entities are required to operate. This ownership and control make CTA vulnerable to Chinese government requests to misuse customer data in a manner that would compromise U.S. national security and law enforcement efforts. As noted above, ODNI identifies the Chinese government as a significant espionage threat to the United States.[352] The customer information that CTA can access through CDRs and SIM cards and other means could provide sensitive and significant details to CTA, its parent entities, and the Chinese government, facilitating their ability to engage in information collection activities for the purpose of espionage against U.S. targets, or for any other activities that are contrary to the protection of U.S. customer records and U.S. interests. The record offers no argument or evidence to refute these concerns.

78. Accordingly, we reject CTA's request to allow it to exclude MVNO service from any revocation or termination order and to continue to operate as an MVNO service provider in the United States.[353] We find unpersuasive CTA's argument that the Commission should allow CTA to continue its provision of MVNO service "given the potential harm to customers from discontinuance of service and the lack of any potential harm from continuing service,"[354] because, as noted above, the potential harm is in fact significant. Allowing CTA to continue to offer MVNO services would be contrary to the national security and law enforcement interests of the United States.

(ii) IPLC, IEPL, and MPLS VPN

79. We find that other services provided by CTA pursuant to its section 214 authority also provide substantial opportunities for CTA to access, monitor, store, disrupt, and/or misroute U.S. communications, and therefore present significant national security and law enforcement risks. Significantly, the Executive Branch agencies note that CTA's international section 214 authorizations "furnish [CTA] with access to more customers, communications traffic, and interconnections with other U.S. common carriers than it would have otherwise."[355] The services that CTA provides pursuant to its section 214 authority include IPLC, IEPL, and MPLS VPN services. Both IPLC and IEPL are lower layer network services that support point-to-point communications.[356] CTA states that its MPLS VPN

(Continued from previous page)
customers); *see infra* note 478 ({[

]}).

[351] *Institution Order*, 35 FCC Rcd at 15025-26, paras 32-33.

[352] *See supra* para. 67.

[353] CTA Mar. 1, 2021 Reply at 60-62.

[354] *Id*. at 62.

[355] Executive Branch Recommendation to Revoke and Terminate at 41-42.

[356] CTA explains that its IPLC service "is a service operating on part of China Telecommunications Corporation's ('CT's') global transmission network providing cross-border or cross-regional customers with fully transparent end-to-end international private dedicated circuit services with fixed bandwidth guarantees for an exclusive end customer." CTA June 8, 2020 Response, Exh. 6 at 3. CTA adds that its IEPL service is "a point-to-point or point-
(continued….)

service "rides on CT's [MPLS] based bearer network called CN2 and interconnected carriers' MPLS networks" and "provides customers with highly secured data transmission for logical connectivity among multiple destinations."[357]

80. CTA is able to combine its IPLC, IEPL, and MPLS VPN section 214 services[358] with its services that do not require section 214 authority to form a suite of services,[359] which further presents opportunities for CTA to engage in activities that undermine the security of the United States. For example, CTA could offer IPLC, IEPL, and MPLS VPN section 214 services individually or combined with other services as part of its MSP offering.[360] In fact, we observe that CTA currently promotes packages that integrate network services provided by its indirect parent CT, and emphasizes on its webpage the international connections offered by CT.[361] For example, CTA states that "China Telecom operates 456 on-net data centers in Mainland China and has a footprint in 187 data centers across 71 key metro hubs globally. From 100+ global [Points of Presence] we are able to provide a variety of Layer 2 and 3 access options to China Telecom's backbone networks."[362] CTA's provision of these services, combined with its relationship to CT 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, CTA can access, monitor, store, disrupt and/or misroute U.S. communications without authorization, which in turn threatens the security and integrity of such communications.

(Continued from previous page)
to-multipoint Ethernet services that provide flexible bandwidth and Ethernet access capabilities over a part of CT's transmission network, or with the interconnected partners' Ethernet network." *Id.*

[357] *Id.*, Exh. 6 at 4.

[358] *See id.*, Exh. 6 at 2-4.

[359] *See* Oracle Corporation, *Open Systems Interconnect Reference Model*, https://docs.oracle.com/cd/E19455-01/806-1017/6jab5di2d/index html (defining the seven layers of networking based on the Open Systems Interconnect reference model, with Internet Protocol (IP) listed at Layer 3 and Ethernet listed at Layer 2); *see also* China Telecom Americas, *Private Leased Circuits*, https://www.ctamericas.com/products-services/data-networking/private-leased-circuits/ (last visited Sept. 22, 2021) (describing IPLC as a "Layer 1 (TDM) network service").

[360] *See* CTA's June 8, 2020 Response, Exh. 6 at 1-4, 8; China Telecom (Americas) Corporation, *China Telecom Ranks Global No. 1 in IR Magazine's Global Top 50 Awards 2017* (Oct. 20, 2017), https://www.ctamericas.com /category/news/ (stating, with regard to its collection of services, "China Telecom Americas provides locally based, one-stop-shop, turnkey solutions for everything from China domestic and international data circuits to IDC services, network management, equipment management, system integration, and much more"); *CTA Product Overview* at 2.

[361] *See* CTA June 8, 2020 Response, Exh. 6 at 3 ("CTA offers [IEPL] . . . over a part of CT's transmission network"); *see, e.g.*, China Telecom (Americas) Corporation, *Ethernet Private Lines*, https://www.ctamericas.com/products-services/data-networking/ethernet-private-lines/ (last visited Sept. 30, 2021); China Telecom (Americas) Corporation, *Global Data Center Map*, https://www.ctamericas.com/global-data-center-map/ (last visited Sept. 22, 2021) (*CTA Global Data Center Map*). CTA's webpage titled "Ethernet Private Lines" promotes both "CTA IEPL service" and "China Telecom's EPL service," and states, "[a]s bandwidth demands grow, multinational enterprises doing business in China require secure, reliable networks that combine operational flexibility with bottom line cost-effectiveness. Ethernet Private Lines let you do just that, with dedicated point-to-point connectivity through China Telecom's next-generation carrier network and access to our high-speed global networks." China Telecom (Americas) Corporation, *Ethernet Private Lines*, https://www.ctamericas.com/products-services/data-networking/ethernet-private-lines/ (last visited Sept. 30, 2021). The same webpage also states, "China Telecom Americas' suite of Ethernet-based private line network services were developed specifically to meet the performance, speed and security demands of both enterprise and carrier customers." *Id.*

[362] *See CTA Global Data Center Map*. As reflected by the quoted language on the webpage titled "Global Data Center Map," CTA's webpages refer to "China Telecom" as the global provider of the "backbone networks" to which CTA connects. *See id.*; *CTA Global Network*; *see also supra* note 321 (discussing CTA's webpages that refer to "China Telecom" in association with CT).

81. 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 the routers, switches, and/or servers (the devices) that store or forward traffic through their network.[363] Bad 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 and/or other deliberate disruption of data and control of signaling operations, such as denial of service in the target's network(s);[364] and (2) passive attacks, involving eavesdropping and monitoring of data to collect information.[365] Active attack intrusions tend to exploit weaknesses in standardized protocols and their implementation.[366] In the case of active attacks, bad actors, including any ISPs, can gain unauthorized access to a victim's data (e.g., through Border Gateway Protocol (BGP) hijacking)[367] from other locations of the Internet to extract metadata or other information or to manipulate the data.[368] In the case of passive attacks, an ISP, for example, can take advantage of its ability as a service provider to carry customer traffic and exploit the trust of its customers and other ISPs that send it traffic by monitoring, observing, and collecting customers' data and/or metadata from such traffic. Passive monitoring can compromise both unencrypted and encrypted traffic.[369] In particular, passive

[363] *See* Karen Scarfone & Peter Mell, National Institute of Standards and Technology (NIST), Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94 (2007), https://csrc nist.gov/publications/detail/sp/800-94/final (*NIST Guide to Intrusion*) (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://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-211.pdf.

[364] *See, e.g.*, Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage* (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).

[365] *See* Richard Derbyshire et al., *An Analysis of Cyber Security Attack Taxonomies* (2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), at 153, 155, 157) (2018), https://ieeexplore.ieee.org/document/8406575; Chris Simmons et al., *AVOIDIT: A Cyber Attack Taxonomy* (2009), at 1-2, https://nsarchive.gwu.edu/sites/default/files/documents/4530310/Chris-Simmons-Charles-Ellis-Sajjan-Shiva.pdf; *see also* Ismail BuTun et al., *Security of the Internet of Things: Vulnerabilities, Attacks, and Countermeasures* (IEEE Communications Surveys & Tutorials, Vol. 22, Issue 1, at 617, 619-622) (2020).

[366] *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, at 404-416) (2019), https://doi.org/10.1145/3307334.3326082 (addressing one example of an exploitation of a network standard and its implementation); Cybersecurity & Infrastructure Security Agency, *Alert (TA16-288A)—Heightened DDoS Threat Posed by Mirai and Other Botnets* (revised Oct. 17, 2017), https://us-cert.cisa.gov/ncas/alerts/TA16-288A (describing Mirai malware that scans the Internet for vulnerable Internet of Things (IoT) devices with weak security that can be incorporated into a botnet for distributed denial-of-service attacks).

[367] *See, e.g., infra* paras. 83-90 (discussing BGP hijacking).

[368] *See, e.g.*, Henry Birge-Lee et al., Bamboozling Certificate Authorities with BGP (SEC'18: Proceedings of the 27th USENIX Conference on Security Symposium, at 833–849) (2018), https://www.princeton.edu/~pmittal/publications/bgp-tls-usenix18.pdf (also available at https://dl.acm.org/doi/10.5555/3277203.3277266).

[369] 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 (continued….)

monitoring can turn into a more serious form of covert surveillance called "pervasive monitoring," which network service providers are well-situated to perform.[370] For example, as part of network management—particularly security management—an ISP, such as CTA, can use tools to identify network intrusion[371] or perform deep packet inspection in the absence of encryption.[372] These tools can be leveraged to further enable CTA 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.

82. As discussed below, CTA's ability, as an ISP, to conduct active attacks and passive monitoring raises significant risks associated with its IPLC, IEPL, and MPLS VPN services. With respect to passive monitoring, CTA 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. CTA has the ability to conduct passive monitoring through its IPLC and IEPL services, which could provide CTA with access to raw data, including their content, in cases where its customers have not incorporated an additional level of end-to-end encryption.[373] With respect to its MPLS VPN service, CTA has the ability, by using the equipment of its customers and/or misrouting, to collect traffic

(Continued from previous page)
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), at 1-5, 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, at 759-776) (2020), https://www.usenix.org/system/files/nsdi20-paper-kwon.pdf; TechTarget, *brute force attack*, https://searchsecurity.techtarget.com/definition/brute-force-cracking.

[370] 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"); *see also* Dana Polatin-Reuben, *Pervasive Monitoring as an Insider Threat* (Human Aspects of Information Security, Privacy, and Trust, at 242-251) (July 2015), https://link.springer.com/chapter/10.1007/978-3-319-20376-8_22. In addition, 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 (Privacy Considerations for Internet Protocols). 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. *Privacy Considerations for Internet Protocols*, at 7, 11-12.

[371] *See, e.g., NIST Guide to Intrusion*.

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

[373] *See* CTA's June 8, 2020 Response, Exh. 16 at 3-4 (stating, "[i]n addition, CTA's enterprise customers are generally sophisticated users that encrypt their data before ever presenting it to CTA"). While 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.

that traverses its network, derive metadata[374] from this traffic, and attempt to decrypt client-encrypted traffic to access the content at a time and location of CTA's choosing.

83. *CTA's Role in Internet Routing and Threats Associated with Services Provided Pursuant to Section 214 Authority.* In addition to active attacks and passive monitoring of networks, CTA's Internet routing operations ultimately present national security and law enforcement risks associated with its IPLC, IEPL, and MPLS VPN services. CTA argues that the Executive Branch agencies' allegations concerning opportunities to disrupt and misroute U.S. communications traffic "relate to CTA's Internet traffic exchange services, which are information services and therefore would not be affected by the proposed revocation of the company's section 214 authorizations."[375] We recognize that forwarding of IP traffic and BGP routing do not require section 214 authority and could continue to be offered by CTA or CT 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 include MPLS VPN service, with regard to IP traffic sent to CTA's network, and potentially IPLC and IEPL services depending on CTA's internal deployment of these services. Additionally, CTA, like any ISP, can monitor its customers' traffic. CTA's provision of a full suite of services heightens the national security and law enforcement risks presented by its ability to monitor customers' traffic, given the expanded potential for customers to utilize CTA's offerings for increased types of communications services. We find that revocation of CTA's section 214 authority therefore could substantially diminish CTA's ability to engage in conduct harmful to the national security and law enforcement interests of the United States.

84. As an initial matter, the risks associated with CTA's role in Internet routing, like the risks associated with any similarly situated ISP, derive from CTA's ability to facilitate espionage and other activities harmful to the national security and law enforcement interests of the United States. CTA claims that the Executive Branch agencies' "description of routing issues is fundamentally misleading, and represents either a failure to understand or a misrepresentation of basic principles of Internet architecture and routing."[376] CTA argues that "in reality, internet routing problems are common and occur on all networks despite the best efforts of responsible operators."[377] However, CTA has offered no persuasive argument to dispel the significant concerns raised in the *Institution Order* that "CTA's argument simply ignores the important role played by service providers in lessening the impacts of such routing issues."[378] CTA also does not dispel the concerns identified by the Executive Branch agencies that CTA's "U.S. operations present opportunities, and plausible deniability, for Chinese state-sponsored actors to disrupt

[374] *See* Joseph Cox, *How Data Brokers Sell Access to the Backbone of the Internet* (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).

[375] CTA June 8, 2020 Response, Exh. 16 at 60, n.141 (citing *Restoring Internet Freedom*, 33 FCC Rcd 311, 410, para. 166 (2018)).

[376] *Id.*, Exh. 16 at 60.

[377] *Id.*, Exh. 16 at 61.

[378] *Institution Order*, 35 FCC Rcd at 15024-25, para. 31 & n.121; *see* Executive Branch Recommendation to Revoke and Terminate at 45 ("Isolated incidents of misrouting, if quickly identified and corrected, may have limited impact. But that is not the case for [CTA]. For nearly a decade, [CTA] has been on notice that its network advertised incorrect routing information to its neighbors on the Internet."). The Executive Branch agencies state, "In today's national security environment, [CTA's] access to the U.S. communications network, and its failure to monitor its network, creates a vulnerability that is just as real as failing to monitor flammable fumes on a factory floor. [CTA's] U.S. operations present opportunities, and plausible deniability, for Chinese state-sponsored actors to disrupt and misroute U.S. Internet traffic." *See* CTA June 8, 2020 Response, Exh. 16 at 61 (quoting Executive Branch Recommendation to Revoke and Terminate at 49); Executive Branch Recommendation to Revoke and Terminate at 49.

and misroute U.S. Internet traffic."[379] For instance, misrouting may occur due to routers deliberately configured to implement a routing architecture that facilitates unauthorized data access. CTA, like any ISP, uses standard routing protocols such as BGP,[380] as well as intra-domain protocols such as Interior Gateway Protocols (IGPs)[381] within its autonomous domains, to route traffic end-to-end across the Internet. Based on analysis of publicly available BGP data,[382] we observe that CTA's network appears to currently have three transit providers, including "China Telecom."[383] CTA and CT can use their BGP peering policies[384] to redirect traffic originally destined to CTA's IP address prefixes in the United States[385] to instead traverse CT's network outside the United States.

[379] Executive Branch Recommendation to Revoke and Terminate at 49.

[380] *See id*. at 45, n.159 ("Much like a GPS navigation system, the BGP routing protocol provides directions for individual packets of data traveling across independently operated networks on the Internet. BGP uses an Autonomous System (AS) architecture, under which each autonomous system (such as a network operated by a university or Internet Service Provider) is assigned a unique Autonomous System Number (ASN). Under BGP, these ASNs collect routing information from their neighboring ASNs (peers) about what routes are available at that moment, and then propagate that routing information further, which results in creating dynamically updated information about available routes on the Internet."); *see also Network Working Group, Request for Comments: 4271, Category: Standards Track, A Border Gateway Protocol 4 (BGP-4)* (Jan. 2006), https://www.rfc-editor.org/info/rfc4271.

[381] An example of IGP is Open Shortest Path First (OSPF). *See Network Working Group, Request for Comments: 2328, Category: Standards Track, OSPF Version 2* (April 1998), https://datatracker.ietf.org/doc/html/rfc2328. We note that an IGP is used to forward traffic between any two points within an ISP or enterprise network.

[382] *See* Hurricane Electric Internet Services, AS36678 China Telecom (Americas) Corporation—AS36678 IPv4 Route Propagation, https://bgp he net/AS36678#_graph4 (last visited Oct. 2, 2021) (*Hurricane Electric Internet Services, AS36678*).

[383] *See* CAIDA, *AS 36678—CTUSA* (Aug. 1, 2021), https://asrank.caida.org/asns?asn=36678&type=search (identifying "China Telecom," "Level 3 Parent, LLC," and "Telia Company AB" as transit providers in association with "CTUSA").

[384] *See* ThousandEyes, *Peering Policy—Peering Policy Overview and Technical Requirements*, https://www.thousandeyes.com/learning/techtorials/peering-policy (last visited Sept. 22, 2021) (explaining peering policies, which are criteria to determine the networks with which an ISP interconnects or peers with other ISPs, and their use by network operators, including BGP routing).

[385] CTA 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/ (last visited Oct. 1, 2021) (search for 66.102.241.10; 104.192.111.10, 69.163.96.10). 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)* (March 1996), https://datatracker.ietf.org/doc/html/rfc1930#section-3 (Sec. 3. Definitions). Based on the ARIN website, "China Telecom (Americas) Corporation" is identified as the name of the Organization ("Org") who is assigned each resource as of the most recent date (April 29, 2020) when the Organization information associated with each IP address prefix was last updated. *See* American Registry for Internet Numbers (ARIN), *ARIN Whois/RDAP—Network: NET-66-102-241-0-1*, https://search.arin.net/rdap/?query=66.102.241.10 (last visited Oct. 1, 2021) (*Network: NET-66-102-241-0-1*); American Registry for Internet Numbers (ARIN), *ARIN Whois/RDAP—Network: NET-104-192-111-0-1*, https://search.arin.net/rdap/?query=104.192.111.10 (last visited Oct. 1, 2021) (*Network: NET-104-192-111-0-1*); American Registry for Internet Numbers (ARIN), *ARIN Whois/RDAP—Network: NET-69-163-96-0-2*, https://search.arin.net/rdap/?query=69.163.96.10 (last visited Oct. 1, 2021) (*Network: NET-69-163-96-0-2*); American Registry for Internet Numbers (ARIN), *Using Whois*, https://www.arin.net/resources/registry/whois/ (last visited Oct. 1, 2021); *see* American Registry for Internet Numbers (ARIN), *Number Resource Policy Manual* (Aug. 12, 2021), https://www.arin.net/participate/policy/nrpm/ (see section 2.5 "Allocation, Assignment, Reallocation, Reassignment"). We observe that the Points of Contact with respect to each IP address prefix include, as of July 2, 2021, an individual whose contact information is associated with CTG, an affiliate of CTA and an

(continued….)

85. Importantly, CTA and CT's BGP peering policies 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.[386] The risks associated with misrouting of and any unauthorized access to such traffic are particularly significant because such activities would not be readily detected by CTA's customers or by end users that may send traffic to CTA's customers. To ascertain any misrouting of Internet traffic, CTA's customers would need to conduct periodic Traceroutes.[387] This threat of misrouting exists because CT, while transmitting the traffic sent to it by CTA, could engage in unauthorized access or copying either by using CT's facilities within the United States[388] 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, then 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 is routed outside of the United States during transit, may be a form of misrouting that raises significant national security and law enforcement concerns.

86. We recognize that an ISP's decisions regarding BGP peering policies result in different routes across the Internet, and the choice of these policies may result in traffic transiting through networks that do not have the same protections of data that exist in the United States. For example, CTA's BGP peering policies may result in data transiting CT's network before it reaches CTA. In rare cases, an Autonomous Systems (AS) can announce false information that deliberately diverts traffic away from normal BGP routes. This is known as "BGP hijacking" or "route leaks."[389] 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"[390] traffic to the customer. Both incidents may occur on either an intentional (i.e., malicious) or accidental basis, and it may be impossible to distinguish between them.[391] This in turn makes it easier to claim that a BGP hijack

(Continued from previous page)
indirect subsidiary of CT. *See Network: NET-66-102-241-0-1*; *Network: NET-104-192-111-0-1*; *Network: NET-69-163-96-0-2*.

[386] If traffic to or from CTA's network is routed via CT's network, the traffic can travel anywhere on CT's network while in transit.

[387] 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 Sept. 22, 2021).

[388] *See* PeeringDB, *China Telecom*, https://www.peeringdb.com/net/308 (last visited Sept. 22, 2021) (*PeeringDB China Telecom*) (identifying public peering exchange points and private peering facilities associated with "China Telecom" (ASN 4134) that include locations in the United States).

[389] *See* Internet Engineering Task Force (IETF), *Request for Comments: 7908, Category: Informational, Problem Definition and Classification of BGP Route Leaks* (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*.

[390] A route blackhole occurs when traffic never reaches its destination. *See, e.g.*, Youtube and Pakistan Telecom, https://youtu.be/IzLPKuAOe50; Hari Balakrishnan, How YouTube was "Hijacked," at 1 (May 2009), http://web mit.edu/6.02/www/s2012/handouts/youtube-pt.pdf.

[391] We observe that 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 RPKI Monitor. *See* NIST, *NIST RPKI Deployment Monitor* (updated Apr. 27, 2021), https://www nist.gov/services-resources/software/nist-rpki-deployment-monitor. *See also* UKNOF 45 Meeting, January 2020, https://www.youtube.com/watch?v=j-
(continued….)

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.[392] 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).[393]

87. The potential for misrouting is influenced by the physical proximity of the provider. If a BGP route announcement for a destination in the United States occurs far away geographically (and topologically from the perspective of BGP), networks in the United States may ignore the announcement, since by the time the announcement reaches a U.S. network, the "hop count"—that is, the number of networks that the traffic must traverse—will be excessively large compared to other routes and thus the announcement would not be used. In contrast, if an anomalous BGP route announcement occurs at a Point of Presence (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, which can cause harm to networks that are topologically closely interconnected to the announcer. In such circumstances, given that there is a greater number of U.S networks that are potentially available to peer within the United States, rather than outside it, this physical proximity in the United States provides CTA with greater opportunity for access to U.S. communications and thus poses a greater national security and law enforcement risk.

88. The Executive Branch agencies express concern that "[f]or nearly a decade, [CTA] has been on notice that its network advertised incorrect routing information to its neighbors on the Internet."[394] The Executive Branch agencies refer to public reports that CTA's network misrouted large amounts of information and communications traffic over long periods, often several months,[395] sometimes involving U.S. government traffic.[396] Whether or not CTA, or its indirect parent CT, engaged in such misrouting either accidentally or intentionally, the record clearly demonstrates that U.S. communications traffic was diverted to China. This diversion of U.S. communications traffic presents significant and

(Continued from previous page)
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 Quantify the Pitfalls of Using Traceroute in AS-Level Topology Measurement* (IEEE Journal on Selected Areas in Communications, Vol. 29, Issue 9, at 1822-24) (Oct. 2011), https://ieeexplore.ieee.org/document/6027864.

[392] *See* Executive Branch Response, Exh. 128 at EB-2974, PSI Report at 66 (noting how certain traffic incidents could allow a carrier to "'compromise the integrity of supposedly secure encrypted communications'") (citing U.S.-CHINA ECON. & SEC. REVIEW COMM'N, REPORT TO CONGRESS 1, 244 (2010)).

[393] *See* Yixin Sun et al., *Securing Internet Applications from Routing Attacks* (Communications of the ACM, Vol. 64 No. 6, at 86-96) (2021), https://cacm.acm.org/magazines/2021/6/252822-securing-internet-applications-from-routing-attacks/fulltext; Tor Project, Inc., https://www.torproject.org (last visited Sept. 22, 2021).

[394] Executive Branch Recommendation to Revoke and Terminate at 45.

[395] *Id*.; *Institution Order*, 35 FCC Rcd at 15024-25, para. 31 & n.121.

[396] *Institution Order*, 35 FCC Rcd at 15024-25, para. 31 & n.122 (citing Executive Branch Recommendation to Revoke and Terminate at 45). The Executive Branch agencies identify 10 examples of such reported incidents. *See* Executive Branch Recommendation to Revoke and Terminate at 45-47. The Executive Branch agencies state that "[w]hen asked to explain, [CTA] claimed that {[

]} *Id*. at 47-48 (quoting *id.*, Business Confidential Exh. 78 at EB-1892, EB-1893, Attachment to E-mail from Morgan Lewis to DOJ National Security Division (Jan. 23, 2019)) (alteration in original).

substantial risks to the security of the United States. CTA, at any given time, has the opportunity to misroute traffic outside of the United States, which raises serious concerns given CTA's ultimate ownership and control by the Chinese government. We remain concerned about the threats involving possible misrouting of communications traffic and related cyber threats identified by the Executive Branch agencies, and CTA has provided no arguments or evidence that dispel these concerns. We find that our concerns about CTA's routing arrangements are not misplaced, and that CTA, through its presence at physical locations in the United States, has opportunity to use its network architecture to engage in activities that adversely affect U.S. communications and the national security and law enforcement interests of the United States.

89. CTA argues that it and its parent entities "strive to implement the best practices for routing security" by, for example, joining the Internet Society's Mutually Agreed Norms for Routing Security (MANRS).[397] MANRS sets out a framework of best practices for network operators to, among other things, prevent route hijacks and leaks.[398] On December 15, 2020, CTA filed with the Commission a letter stating that, "[o]n December 10, 2020, CTA announced that CTA, China Telecom, and China Telecom (Global) had been accepted into MANRS."[399] We find that membership in MANRS does not overcome the significant threats posed by CTA to the national security and law enforcement interests of the United States. While MANRS provides a set of best practices and guidelines for promoting security in Internet routing, these measures are selected from a variety of options to be incremental and low cost;[400] only as effective as the commitment of all concerned ISPs in adopting them; and subject to any limitations in the scope of protection that the aforementioned practices afford. MANRS cannot ensure that all providers that may peer with CT or CTA implement its recommendations. More importantly, despite years spent developing the relevant standards, the intrinsic security flaws in BGP are still not

[397] Letter from Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP, to Marlene H. Dortch, Secretary, FCC, at 2 and Exh. A (Dec. 15, 2020) (on file in GN Docket No. 20-109; IB File Nos. ITC-214-20010613-00346; ITC-214-20020716-00371; and ITC-T/C-20070725-00285) (CTA Dec. 15, 2020 Letter); *see also* CTA June 8, 2020 Response, Exh. 16 at 62-63.

[398] *See* Mutually Agreed Norms for Routing Security (MANRS), *MANRS for Network Operators* (May 17, 2021), https://www.manrs.org/isps/ (MANRS/ISPs) ("Mutually Agreed Norms for Routing Security (MANRS) is an initiative to greatly improve the security and resilience of the Internet's global routing system. It does this by encouraging those running BGP to implement well-established industry best practices and technological solutions that can address the most common threats."); Mutually Agreed Norms for Routing Security (MANRS), *Mutually Agreed Norms for Routing Security*, https://www manrs.org/ (last visited Sept. 27, 2021); Internet Society, *MANRS—Mutually Agreed Norms for Routing Security*, https://www.internetsociety.org/issues/manrs/ (last visited Sept. 22, 2021); Mutually Agreed Norms for Routing Security (MANRS), *About*, https://observatory.manrs.org/#/about (last visited Sept. 22, 2021). MANRS has recently developed aids to visualize and quantify observed routing incidents. Known as the MANRS Observatory, this project of MANRS uses publicly available data to track routing incidents and provide an overview of global routing security. *See* Mutually Agreed Norms for Routing Security (MANRS), *Overview*, https://observatory manrs.org/#/overview (last visited Sept. 22, 2021). *See also* Fred Baker, Internet Routing with MANRS, at 2, https://www.manrs.org/wp-content/uploads/2018/11/Internet-Routing-with-MANRS.pdf ("Customers trust that their ISPs and IXPs will connect them to those entities with whom they want to communicate. Routing incidents, such as accepting or propagating a false prefix, are a fundamental service failure in that they connect their customers to someone else.").

[399] CTA Dec. 15, 2020 Letter at 2. According to CTA, "China Telecom's backbone network AS4134 is accepted into the MANRS and the remainder of China Telecom's backbone networks, AS4809, is in the implementation process and expected to meet the same standards in 2021." *Id.* at 2, n.7; *see also* Press Release, China Telecom (Americas) Corporation, *All China Telecom Backbone Networks Accepted by MANRS* (June 1, 2021), https://www.ctamericas.com/all-china-telecom-backbone-networks-accepted-by-manrs/ (stating "[t]he four China Telecom networks accepted by MANRS to date are AS4134, AS4809, AS23764 and AS36678.").

[400] *See MANRS/ISPs.*

resolved in actual deployments.[401] We further add that the Chinese government, through its ultimate ownership and control of CTA, can influence CTA to act upon the opportunities discussed above, which MANRS membership will not prevent. CTA's vulnerability to Chinese government influence therefore presents an unacceptable risk to U.S. communications. We find that CTA's role and capabilities as a network service provider, combined with its physical presence in the United States and its ultimate ownership by the Chinese government, makes the national security and law enforcement risks especially significant.

90. 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."[402] Individuals, companies, and anyone else using CTA's network services entrust their data and communications to CTA, 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."[403] The situation remains applicable today; in its privileged role as a network service provider, and with a physical presence in the United States, combined with its section 214 authorized and other services, CTA has access to sensitive and valuable communications network and customer information and with this information can engage in malicious activity. This includes both active attacks and passive or pervasive monitoring and these activities are not easily discoverable, as described above.[404] Given our concerns, revocation of CTA's domestic and international section 214 authority will diminish and limit, if not cause CTA to remove entirely, its physical presence in the United States and, accordingly, reduce its ability and opportunity to access, store, monitor, disrupt, and/or misroute U.S. communications.

91. *Security Threats Related to CTA's Physical Presence in the United States.* A key measure of an international network service provider's physical span or reach is the number and

---

[401] *See* Lychev, Robert, Sharon Goldberg, & Michael Schapira, BGP Security in Partial Deployment—Is the Juice Worth the Squeeze? (SIGCOMM'13) (2013), https://www.cs.bu.edu/~goldbe/papers/partialSec.pdf; *see also* Qi Li et al., Even Rockets Cannot Make Pigs Fly Sustainably: Can BGP Be Secured with BGPsec?, https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/86415/eth-8844-01.pdf?sequence=1&isAllowed=y.

[402] 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) (Paul Ohm Statement); *see also NIST Guide to Intrusion (*discussion on Deep Packet Inspection).

[403] *Coggs v. Bernard*, 2 Ld Raym 909, 918, 92 ER 107 (1703) (a historical case issued in 1703 recognizing the unique trust relationship between customers and 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); Oliver Wendell Holmes, The Common Law: The Bailee at Common Law, at 164 (1881); Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (discussing users' lack of trust in the security of their data and communications on the Internet).

[404] *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://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf (discussing the data that can be gathered by a network service provider from its customers and end users).

distribution of its PoPs, which are physical locations where the network service provider offers or avails of interconnection or other Internet-related services. To optimize connectivity among providers, the industry has established "Internet Exchange" or "IX" points, which are physical data centers in which carriers who wish to participate in public peering can connect to a shared local area network or optionally avail of point-to-point interconnects for private peering.[405] BGP routes are exchanged between providers that enter into agreements to this end. In cases where CTA's PoPs reside in IX points,[406] CTA can potentially access and/or manipulate data where it is on the preferred path for U.S. customer traffic, through its services provided pursuant to section 214 authority and those services not authorized under section 214 authority. This access to data exists regardless of whether malicious or accidental BGP route manipulation has occurred. In particular, CTA's MPLS VPN service involves the use of PoPs to interconnect with other providers using BGP routers.

92. We agree with the Executive Branch agencies that CTA's PoPs in the United States are highly relevant to the national security and law enforcement risks associated with CTA because "[CTA's] U.S. operations, particularly its eighteen (18) Points of Presence (PoPs) in the United States, provide Chinese government-sponsored actors with openings to disrupt and misroute U.S. data and communications traffic."[407] CTA's website, which reflected in 2019 that CTA had 18 PoPs in the United States,[408] shows that, two years later, CTA presently has 23 PoPs in the United States.[409] CTA's PoPs in the United States are not separate operations unrelated to the various services that CTA offers pursuant to section 214 authority. Rather, CTA's PoPs in the United States provide CTA with the capability to misroute traffic and, in so doing, access and/or manipulate that traffic.

93. In addition, in the course of providing services pursuant to its section 214 authority, including IPLC and IEPL services, CTA, like any similarly situated provider, can have both physical and remote access to its customers' equipment needed to provide such services. This physical access to customers' equipment would allow CTA to monitor and record sensitive information. Further, as the *Institution Order* stated, "[e]vent if, for any reason, CTA had no access to a customer's equipment and simply monitored connectivity over the network it uses to serve that customer, any monitoring of connectivity and transmission can provide substantial, and highly valuable, information that could

[405] We note that private peering can also occur outside IXPs, at data centers referred to as "carrier hotels" or "colocation points." *See, e.g.*, Michael Levy, *What are "Carrier Hotels" and Why Are They Valuable to Your Business?* (May 28, 2019), https://www.rackspace.com/blog/carrier-hotels-are-valuable-to-your-business.

[406] According to PeeringDB's webpage associated with "China Telecom" (reflected as "Organization") and "CTA" (reflected as "Also Known As"), CTA is available for private peering at several facilities. *See Peering DB CTANET*.

[407] Executive Branch Recommendation to Revoke and Terminate at 44 (citing *id.*, Exh. 6 at EB-296-331, Compiled list of [CTA's] U.S. PoPs (Points of Presence), Colocation facilities and Cloud Exchanges and screenshots of Global Data Center Map, https://www.ctamericas.com/global-data-center-map/ (accessed Feb. 1, 2019)); *see PeeringDB CTANET* (identifying, in association with ASN 36678, three PoPs in the United States where CTA is available for private peering Internet interconnection); PeeringDB, *The Interconnection Database*, https://www.peeringdb.com/ (last visited Oct. 1, 2021) (stating, "PeeringDB is a freely available, user-maintained, database of networks" and interconnection data and "facilitates the global interconnection of networks at Internet Exchange Points (IXPs), data centers, and other interconnection facilities").

[408] *See* Executive Branch Recommendation to Revoke and Terminate at 44 (citing *id.*, Exh. 6 at EB-296-331, Compiled list of [CTA's] U.S. PoPs (Points of Presence), Colocation facilities and Cloud Exchanges and screenshots of Global Data Center Map, https://www.ctamericas.com/global-data-center-map/ (accessed Feb. 1, 2019)).

[409] *See CTA Global Data Center Map* (displaying 26 results, as of October 2, 2021, on the "Global Data Center Map" that are associated with "POP" in North America, including 3 locations in Canada as well as 1 location in the United States that is solely labeled as a "COLO" and is not identified as a "POP" in the related description).

potentially be used for espionage."[410] CTA states, for example, that its MSP service "does not have access to any customer-owned equipment unless the customer authorizes that access for trouble-shooting purposes."[411] This does not negate CTA's ability and opportunity to leverage its physical access in ways that cause harm to U.S. communications, and we consider this to be a serious risk. In fact, such opportunities to cause harm in their role of managing customer equipment in support of services pursuant to their section 214 authority, are exactly the opportunities that bad actors seek. We note that DHS' Cybersecurity & Infrastructure Security Agency has received multiple reports of bad actors actively exploiting trust relationships in information technology service provider networks.[412]

94. *Additional Concerns Involving Services Provided by CTA Pursuant to Section 214 Authority*. CTA's MPLS VPN service offering, along with its transit relationship with CT, provides CTA with the ability and opportunity to misroute traffic and/or forward traffic to CT, its indirect parent. CT, acting on its ability and opportunity, can then forward traffic in ways that are only known by CT, potentially further enabling espionage or other activities contrary to U.S. national security and law enforcement interests. As discussed above, CTA advertises access to part of its network via its indirect parent CT's Internet backbone network, including CN2, highlighting its access to the segment of the Internet within China and interconnections with Chinese carriers.[413]

95. With respect to CTA's IEPL service, the potential for misrouting exists with two mechanisms by which CTA may send traffic: (1) directly between endpoints using a point-to-point Ethernet circuit or (2) over its IP network.[414] The first mechanism, with a point-to-point Ethernet circuit, would require using long-haul transport infrastructure (e.g., fiber) from one of CTA's backbone providers, such as its indirect parent CT.[415] In this case, if CTA uses its parent entity's network, the risks associated with misrouting are those attributable to CT 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

[410] *Institution Order*, 35 FCC Rcd at 15027, para. 35.

[411] CTA June 8, 2020 Response, Exh. 16 at 58.

[412] *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 (last visited Sept. 22, 2021).

[413] *See, e.g.*, CTA June 8, 2020 Response, Exh. 6 at 4; *CTA Global Network* (stating, "China Telecom Americas delivers a comprehensive range of high quality telecommunications services to customers around the world" and "[w]e . . . leverag[e] the strength of our Tier-1 global network built on 48 diverse international cable routes and 87 Points of Presence in key metro areas around the world"); China Telecom (Americas) Corporation, *Global Internet Access*, https://www.ctamericas.com/products-services/internet/global-internet-access/ (last visited Sept. 22, 2021) ("China Telecom's Global Internet Services offers enterprises access to ChinaNet (AS4134) and CN2 ([AS]4809) through a variety of bandwidth speeds and Internet access technologies."); China Telecom (Americas) Corporation, *Global IP Transit*, https://www.ctamericas.com/products-services/internet/global-ip-transit/ (last visited Sept. 22, 2021) (*CTA Global IP Transit*) (stating, "China Telecom's Global IP Transit offers connectivity everywhere around the world via CN2 (AS4809) with highest resiliency, redundancy and low latency."). CTA's webpage titled, "Global IP Transit," further associates the Global IP Transit service with "BGP-4 routing to AS4809 and AS4134." *CTA Global IP Transit*; *see also* PeeringDB, *China Telecom* (updated May 14, 2016), https://www.peeringdb.com/org/425 (identifying "China Telecom's" affiliated networks as ASN 4134 (China Telecom), ASN 4809 (China Telecom/CN2), ASN 36678 (CTANET), and ASN 23764 (CTGNet)). *See Hurricane Electric Internet Services, AS36678*.

[414] Forwarding IEPL traffic over IP networks can be accomplished in several ways. The details of every permutation are not described herein because the end result remains the same.

[415] According to the PeeringDB's database, CT and CTA share a private peering facility in Los Angeles, California. *See PeeringDB China Telecom*; *PeeringDB CTANET*. *See also CTA Global Network*.

above, and require using one of CTA's transit providers, such as its indirect parent CT.[416] 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 pursuant to its section 214 authority, CTA would choose which of these two mechanisms to employ. In the event CTA chooses or is required to pursue either mechanism with involvement by CT, significant risks would follow, as CT could easily and without the knowledge of CTA's customers route U.S. traffic through non-U.S. facilities, including those in China.

96. We also note that, 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 traffic through monitoring ports to capture it or forward it to another destination for eventual capture.[417] In addition, CTA's provision of IPLC, IEPL, and MPLS VPN services, whether provided individually or as part of a package in CTA's MSP service offering, present opportunities to (1) access customer metadata, (2) access customer data including all content, and (3) misroute communications (at layers below IP). Notably, all of these harms could occur without the customer's authorization or knowledge.

97. Regarding the risks of harms from CTA's package of services, and in particular its MSP offering, we are not persuaded by CTA's argument that "[its] business model, including its access to customer data, does not provide what the [Executive Branch] Recommendation suggests as opportunities for economic espionage."[418] Nor are we persuaded by CTA's contention that its MSP service, NetCare, "only monitors connectivity and transmission quality on the CTA-provided circuit, and does not have access to any customer-owned equipment unless the customer authorizes that access for trouble-shooting purposes."[419] CTA provides no evidence that it cannot engage in unauthorized access. Nor does CTA provide sufficient evidence to demonstrate that it is not subject to exploitation, influence, and control by the Chinese government. As a result, we find that CTA cannot be trusted to refrain from engaging in unauthorized access or misuse of customer data at the direction of its parent entities and/or the Chinese government.

98. We find that CTA's provision of the services described above—including those requiring section 214 authority such as MVNO, IPLC, IEPL, and MPLS VPN—raise significant national security and law enforcement risks. We conclude that these services, whether offered individually or as part of a suite of services—combined with CTA's physical presence in the United States, CTA's ultimate ownership and control by the Chinese government,[420] and CTA's relationship with its indirect parent CT, which itself maintains a physical presence in the United States[421]—present unacceptable national security and law enforcement risks to the United States.

---

[416] *See* CTA June 8, 2020 Response, Exh. 6 at 4 ("CTA's Global Internet Service is Internet access and transit services. To provide Global Internet Service, CTA uses both ChinaNet (AS 4134) and CN2 (AS 4809). CTA has its own peering and IP transit, but CTA's network is part of the global ChinaNet and CN2 network."); *see also PeeringDB China Telecom*; Peering DB, *China Telecom/CN2*, https://www.peeringdb.com/net/7941 (last visited Sept. 22, 2021).

[417] *See, e.g.,* Marija Furdek et al., Vulnerabilities and Security Issues in Optical Networks (July 2014), https://www.researchgate net/publication/269268194_Vulnerabilities_and_security_issues_in_optical_networks.

[418] CTA June 8, 2020 Response, Exh. 16 at 57.

[419] *Id*., Exh. 16 at 58.

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

[421] *See supra* note 407 (referencing CTA's U.S. Points of Presence, colocation facilities, and cloud exchanges); *see also PeeringDB China Telecom* (identifying public peering exchange points and private peering facilities associated (continued….)

b. Additional Comments in the Record

99. We are not persuaded by comments filed in the record. According to the Internet Governance Project, "[it has] studied numerous cybersecurity incidents attributed to Chinese actors, including the OMB breach, APT40 intrusions on private industry, the Marriott Hotels breach, Gh0stNet, and others."[422] The Internet Governance Project states that "[i]n none of these cases is there any evidence that Chinese cyber-espionage relied on the presence of China Telecom in the U.S. market. Chinese cyber espionage is not conducted by CTA and does not depend in any way on CTA's section 214 authorizations or on its possession of [International Signaling Point Code (ISPC)] assignments."[423] The Internet Governance Project fails to acknowledge that the incidents it cites represent examples of active attacks of intrusion and do not reflect the passive monitoring of traffic that CTA can conduct. As discussed above, CTA's ability and opportunity to conduct active attacks as well as passive monitoring, combined with its vulnerability to the exploitation, influence, and control by the Chinese government, poses significant national security and law enforcement concerns.[424] We also find unpersuasive Internet Governance Project's contention that the Commission "should reject this effort to bar CTA from access to the US telecommunication services market" because it "is backtracking on its commitment to open entry."[425] The Internet Governance Project provides no persuasive evidence for its claims and fails to refute the evidence regarding the concerns associated with CTA's retention of its section 214 authority. Finally, as noted by some commenters, we recognize that revocation or termination of section 214 authority to provide service may result in costs incurred on customers. However, the generalized arguments submitted by the commenters fail to refute the evidence in the record regarding the substantial and significant national security and law enforcement concerns associated with CTA's retention of its section 214 authority.

3. CTA's Past Conduct and Representations to the FCC and Other U.S. Government Agencies Requires Revocation

100. The overwhelming record evidence concerning CTA's past conduct and representations to the Commission and other U.S. government agencies requires us to find—independent of our separate concerns about the intent and ability of the Chinese government to use its control of CTA 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 CTA's retention of its section 214 authority.[426] CTA's conduct and representations to the Commission and other U.S. government agencies demonstrate a lack of candor, trustworthiness, and reliability that erodes the baseline level of trust that the Commission and

(Continued from previous page)
with "China Telecom," Autonomous System Number 4134); *PeeringDB CTANET*. The PeeringDB's webpage associated with "China Telecom" (ASN 4134) identifies that CT has public peering exchange points in New York and Miami, and identifies private peering facilities in eight locations in the United States. *PeeringDB China Telecom.* The list of facilities reflected on this webpage represents examples of CT's physical presence in the United States and is not exhaustive. *Id*.

[422] Internet Governance Project Comments at 2.

[423] *Id*. *See also* Internet Governance Project *Ex Parte*; Executive Branch Response at 2-3 (noting that CTA's June 8, 2020 Response "presents an unsourced quote by a 'Brendan [sic] Kuerbis' that criticizes media reports linking [CTA] to Internet misrouting incidents" and expressing concern that "[a]dditional research discloses that a 'Brenden Kuerbis' was identified in connection with foreign influence efforts by [CTA], according to a publicly available Department of Justice (DOJ) Foreign Agents Registration Act (FARA) filing"); CTA Mar. 1, 2021 Reply at 52-54 (contending that "the opinions [Mr. Kuerbis of the Internet Governance Project] expressed in September 2019 were entirely consistent with his November 2018 post, which he published months before first being contacted on behalf of CTA.").

[424] *See, e.g.*, *supra* para. 82 & Section III.B.1.

[425] Internet Governance Project Comments at 1.

[426] *Institution Order*, 35 FCC Rcd at 15032, para. 43.

other U.S. government agencies require of telecommunications carriers. As noted above, carriers sit at a privileged position and trust is paramount given the critical nature of the provision of telecommunications service in the United States. Based on the record evidence, CTA cannot be trusted to cooperate with the Executive Branch agencies to ensure compliance with its 2007 LOA, to assist the Commission's implementation of its statutory obligation to act "for the purpose of the national defense [and] for the purpose of promoting safety of life and property,"[427] or to comply with the Commission's implementing rules. Specifically, we find that the record supports the Executive Branch agencies' assessment that CTA failed to disclose to U.S. government authorities critical information concerning where it stored U.S. records. We find that CTA also made inaccurate statements to U.S. government authorities and the Commission about its cybersecurity practices.[428] As discussed below, we also find that CTA failed to notify the Executive Branch agencies of its ISPC filings, a requirement in the 2007 LOA, and failed to comply with the Commission's own ISPC requirements, requiring the Commission to reclaim the ISPCs issued to CTA.[429] CTA's actions concerning ISPCs further affirm our concerns regarding CTA's candor, trustworthiness, and reliability.[430]

101. *U.S. Records.* The record evidence shows that CTA was not transparent and forthright in its representations to the Executive Branch agencies and the Commission concerning U.S. records. CTA is required under the 2007 LOA to, among other things, "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]."[431] This provision in the 2007 LOA is critical in ensuring the protection of communications and U.S. records. Importantly, the Commission's rules and precedent require any holder of a Commission authorization to, among other things, make truthful and accurate statements to the Commission.[432] Specifically, CTA was not truthful with regard to {[ ]}[433]

102. As background, {[

[427] 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.

[428] Executive Branch Recommendation to Revoke and Terminate at 17-26; *see Institution Order*, 35 FCC Rcd at 15029, para. 37.

[429] *See infra* Section III.C.; Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Zhao-feng Ye, Xiaoyi Liu, China Telecom (Americas) Corporation, DA 20-1368 (Nov. 18, 2020) (on file in GN Docket No. 20-109, File Nos. SPC-NEW-20030314-00014, SPC-NEW-20100314-00006, SPC-NEW-20100326-00007, ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285) (ISPC Reclamation Letter).

[430] Related to the discussion here, we also terminate CTA's international section 214 authority for failure to comply with two provisions of the 2007 LOA, an express condition of CTA's international section 214 authorizations below. *See infra* Section III.C.

[431] 2007 LOA at 2; *see Institution Order*, 35 FCC Rcd at 15034-38, paras. 50-54; *see infra* Section III.C.

[432] 47 CFR § 1.17 (prohibiting intentional omissions of material information).

[433] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15, May 11, 2007 Response; *id.*, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter; *id.*, Business Confidential Exh. 103 at EB-2111-13, April 4, 2019 Letter; *Institution Order*, 35 FCC Rcd at 15029-30, 15037-38, paras. 37-39, 54.

[434] As common practice, prior to entering into an LOA with a referred applicant, the Executive Branch agencies "generally initiate review of a referred application by sending the applicant a set of questions seeking further information." *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10929, para. 5; *Institution Order*, 35 FCC Rcd at 15036-37, para. 53. In 2020, the Commission issued the *Executive Branch Process Reform* (continued….)

]} inform Team Telecom if it intends to store *any* U.S. business records outside the United States prior to doing so."[435] Indeed, the Executive Branch agencies relied upon {[ ]} when CTA entered into the 2007 LOA and the agencies subsequently advised the Commission that they had no objection to the Commission granting the transfer of control of CTA's international section 214 authorizations, provided that the Commission condition the grant on CTA's compliance with the 2007 LOA.[436] {[ ]} among other things, "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]."[437] {[

]}[438]

103. Nine years later, CTA voluntarily sent a letter dated January 11, 2016, to the Executive Branch agencies, stating that {[

]}[440] CTA added that, "at times between May 2013 and June 2014, U.S. Records were temporarily stored outside of the U.S. during the transition to the {[

(Continued from previous page)
Report and Order that now requires applicants to file their responses to the questions (now called Standard Questions) directly with the Committee—prior to or at the same time they file their applications with the Commission—to expedite the review process. *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10935, 10942, 10946, paras. 18, 40, 48; *id.* at 10935, para. 18 ("This will enable the Executive Branch agencies to begin their review earlier in the process than is now the case and may eliminate the need to send a specifically tailored questionnaire (Tailored Questions) to each applicant.").

[435] *See* CTA June 8, 2020 Response, Exh. 16 at 38 & n.77 (quoting Executive Branch Recommendation to Revoke and Terminate at 21 and noting citation therein to "Recommendation Exhibit 3 at EB-15") (emphasis added); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15, May 11, 2007 Response (emphasis added). *See also Institution Order*, 35 FCC Rcd at 15029-30, para. 38; Executive Branch Recommendation to Revoke and Terminate at 21. {[ ]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15.

[436] Executive Branch Recommendation to Revoke and Terminate at 21; 2007 LOA; Petition to Adopt Conditions to Authorizations and Licenses at 1-2; *2007 Pro Forma Grant Public Notice*, 22 FCC Rcd at 15268.

[437] *See infra* Section III.C.; 2007 LOA at 2; *Institution Order*, 35 FCC Rcd at 15037-38, para. 54.

[438] Executive Branch Recommendation to Revoke and Terminate at 21; *id.*, Business Confidential Exh. 3 at EB-15, May 11, 2007 Response; *Institution Order*, 35 FCC Rcd at 15037, para. 53. As NTIA explained, "this information is necessary for the Executive Branch's assessment of whether an application raises national security or law enforcement concerns" and assists the Executive Branch agencies to "determine whether it needs to negotiate a mitigation agreement." *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10929, 10943, paras. 5, 42; *see also id.* at 10929, para. 5, n.5; *Institution Order*, 35 FCC Rcd at 15037, para. 53.

[439] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2781, January 11, 2016 Letter.

[440] *Id.*, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter.

]} "[d]uring this entire period, CTA had access to these records and the data was available in the U.S. for response to U.S. process."[441] CTA further stated, "[s]ince June 2014, US Records have been stored in the U.S. in the Company's data center in {[ ]} California."[442]

104. As part of the Executive Branch agencies' compliance review of CTA in 2018,[443] on November 6, 2018, the agencies sent CTA a request asking for "information management policies governing the sharing of U.S. customer information between [CTA] and its ultimate parent company, China Telecom Corporation. For example, how is personally identifiable information from U.S. customers treated and/or accessed?"[444] On December 6, 2018, CTA sent another letter to the Executive Branch agencies in which it responded to this inquiry, among other things, {[

[441] *See* CTA June 8, 2020 Response, Exh. 16 at 37, n.68 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter. In its June 8, 2020 Response to the *Order to Show Cause*, CTA states, "[a]lthough not obligated to do so under the LOA, CTA also informed Team Telecom in 2014 that {
]} During that time, the records were always available to U.S. law enforcement agencies as required under the LOA. In January 2016, this information was formally provided to Team Telecom by letter." CTA June 8, 2020 Response, Exh. 16 at 24-25 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783).

[442] *See* CTA June 8, 2020 Response, Exh. 16 at 37, n.69 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter. In the January 11, 2016 Letter, {[
]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783.

[443] *See* CTA June 8, 2020 Response, Exh. 16 at 26-27; Executive Branch Recommendation to Revoke and Terminate at 17-18; *see infra* para. 111 & note 484.

[444] *See* CTA June 8, 2020 Response, Exh. 16 at 26-27 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-587); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586-587, November 26, 2018 Email.

[445] *See* CTA June 8, 2020 Response, Exh. 16 at 27 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-654); *id.*, Exh. 16 at 40-41 & n.88 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-654); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-590, December 6, 2018 Letter with Attachments.

[446] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments; *id.* at 19 (quoting *id.,* Business Confidential Exh. 36 at EB-624); *Institution Order*, 35 FCC Rcd at 15029, para. 38; *see also* Executive Branch Recommendation to Revoke and Terminate at 25; *id.*, Business Confidential Exh. 96 at EB-2000-2003, March 21, 2019 Letter; *id.*, Business Confidential Exh. 102 at EB-2103-06, March 21, 2019 Letter. {[

(continued….)

]}[451]

105. {[

]}[452] Following this further questioning by the Executive Branch agencies, on April 4, 2019, CTA admitted that "[b]eginning in May 2013, when the {[ ]} was implemented, U.S. records were available to CTA's non-[U.S.] affiliates abroad," but that "[p]rior to 2013, all CTA U.S. Records were retained on CTA servers in Herndon, VA . . . ."[453] {[

]}[454]

(Continued from previous page)

]}

Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-590 (emphasis added).

[447] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-622, EB-634, December 6, 2018 Letter with Attachments.

[448] *Id*., Business Confidential Exh. 36 at EB-623, EB-634, December 6, 2018 Letter with Attachments.

[449] *Id*., Business Confidential Exh. 36 at EB-622, December 6, 2018 Letter with Attachments.

[450] *Id.*

[451] *Id.*, Business Confidential Exh. 36 at EB-623, December 6, 2018 Letter with Attachments. {

]} *Id.*, Business Confidential Exh. 36 at EB-622.

[452] *Id*., Business Confidential Exh. 96 at EB-2000, EB-2002, March 21, 2019 Letter; *id.*, Business Confidential Exh. 102 at EB-2103, EB-2105, March 21, 2019 Letter. {[

]} *Id.*, Business Confidential Exh. 96 at EB-2002; *id.*, Business Confidential Exh. 102 at EB-2105.

[453] *See* CTA June 8, 2020 Response, Exh. 16 at 28 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111, April 4, 2019 Letter; *id.* at 19. *See also Institution Order*, 35 FCC Rcd at 15029, para. 38.

[454] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112, April 4, 2019 Letter; *id.* at 19; CTA June 8, Response, Exh. 16 at 28 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112); *Institution Order*, 35 FCC Rcd at 15029, para. 38. {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 96 at EB-2002, March 21, 2019 Letter; *id.*, Business Confidential 102 at EB-2105, March 21, 2019 Letter; *id.*, Business Confidential Exh. 103 at (continued….)

106. Based on our review of the record, we find that CTA was not truthful and failed to fully disclose to the Executive Branch agencies {[

]}[458] As noted above, CTA represented in its January 11, 2016 Letter that U.S. records were "temporarily stored outside of the U.S. during the transition to the {[ ]} at times between May 2013 and June 2014, but "[s]ince June 2014, US Records have been stored in the U.S. in the Company's data center in {[ ]} California."[459] {[

]}[460]

107. The omissions concerning U.S. records in CTA's representations to the Executive Branch agencies are even more significant {[

(Continued from previous page)
EB-2112. In its June 8, 2020 Response, CTA states that "[it] stated that copies of its U.S. Records for most services were located on the {[ ]} CTA June 8, 2020 Response, Exh. 16 at 28 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112).

[455] *See supra* para. 104 ({[ ]}); *see also* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621-624, EB-634, December 6, 2018 Letter with Attachments. {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2113. The PSI Report states, "CTA also acknowledged that, 'in 2015, CTA new customer information began to be ported onto a web-based platform located in China, with some existing customer data duplicated on this platform,' although it eventually established a U.S-.based data storage system. Team Telecom, however, noted that CTA passed certain customer data to CTG staff 'at overseas network operations centers to manage enterprise data services . . .' and that CTA 'store[d] [U.S.] customer data in the [United States] and Hong Kong.'" Executive Branch Response, Exh. 128 at EB-2972, PSI Report at 64 (citations omitted).

[456] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15, May 11, 2007 Response.

[457] *Id*. ({[ ]}).

[458] *Id*., Business Confidential Exh. 103 at EB-2111-13, April 4, 2019 Letter; *id*., Business Confidential Exh. 36 at EB-621-630, EB-634, December 6, 2018 Letter with Attachments; *see also supra* para. 104 ({[ ]}).

[459] *See* CTA June 8, 2020 Response, Exh. 16 at 37, nn.68-69 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter; *see supra* para. 103.

[460] *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter.

[461] *Id*., Business Confidential Exh. 36 at EB-621, EB-623, EB-628, December 6, 2018 Letter with Attachments.

]}[463]

108. Moreover, we do not give weight to CTA's contention that, at the time CTA sent the January 11, 2016 Letter, "Team Telecom raised no questions {[ ]}[464] or that CTA was not required to provide notice to the Executive Branch agencies prior to making U.S. Records available at non-U.S. locations.[465] In 2016, the Executive Branch agencies {[ ]}[466] We believe this was a reasonable interpretation of CTA's prior statements to the Executive Branch agencies. Indeed, it is CTA's responsibility to affirmatively provide complete information to the Executive Branch agencies in accordance with its commitments to the agencies and to assist the agencies in ensuring the protection of U.S. records.

109. We further find that the distinction that CTA seeks to create between "storage of records" and "access to those records"[467] is unsupported by the record and fails to justify CTA's omissions to the Executive Branch agencies. In fact, CTA's contention that "the Recommendation confuses *storage* of records with *access* to those records"[468] is contradicted by {[

[462] *See id*., Business Confidential Exh. 36 at EB-621, December 6, 2018 Letter with Attachments.

[463] *See id*. {[

]} *Id.*, Business Confidential Exh. 36 at EB-623.

[464] CTA June 8, 2020 Response, Exh. 16 at 25.

[465] *See id*., Exh. 16 at 29 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112, April 4, 2019 Letter. {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 96 at EB-2002, March 21, 2019 Letter; *id.*, Business Confidential Exh. 102 at EB-2105, March 21, 2019 Letter; *id.*, Business Confidential Exh. 103 at EB-2111. CTA responded by stating, "CTA's LOA does not require notice to be provided prior to making U.S. Records available at non-U.S. locations. As such, CTA has not submitted any notification to the DOJ, FBI or DHS prior to making U.S. Records (or copies) available at any non-U.S. location. As you are aware, CTA and Team Telecom have maintained a continuous dialogue on this issue for at least five years." *See* CTA June 8, 2020 Response, Exh. 16 at 29 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112.

[466] *See* Executive Branch Recommendation to Revoke and Terminate at 19-21.

[467] *See* CTA June 8, 2020 Response, Exh. 16 at 38.

[468] *Id*.

]} "at times between May 2013 and June 2014, U.S. Records were *temporarily* stored outside of the U.S. . . . ."[474] This lack of truthfulness to the Executive Branch agencies concerning U.S. records is unacceptable and presents significant national security and law enforcement concerns.

110. CTA had multiple opportunities—whether voluntarily, or in response to the Executive Branch agencies' mitigation monitoring, or in this proceeding—to admit that it failed to disclose to U.S. government authorities critical information {[
]} The record shows {[

[469] *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621-630, EB-634, December 6, 2018 Letter with Attachments; *id.*, Business Confidential Exh. 103 at EB-2111-13, April 4, 2019 Letter.

[470] *Id*., Business Confidential Exh. 36 at EB-621, December 6, 2018 Letter with Attachments (emphasis added).

[471] {[

]} *Institution Order*, 35 FCC Rcd at 15037-38, para. 54, n.214; Executive Branch Recommendation to Revoke and Terminate at 19 (citing *id.*, Business Confidential Exh. 36 at EB-624). {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments (emphasis added). {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624 (emphasis added).

[472] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-623, December 6, 2018 Letter with Attachments.

[473] *Id*., Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments.

[474] *See* CTA June 8, 2020 Response, Exh. 16 at 37, n.68 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783) (emphasis added); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter.

]}[477]
Further, CTA is required to make truthful and accurate statements to the Commission. CTA had the opportunity in this proceeding to admit that it erred, but it did not, which also shows CTA's lack of transparency and forthrightness to the Commission on a critical matter concerning the security and protection of U.S. records.[478]

111. *Cybersecurity Policies*. We also find based on the record that CTA made inaccurate statements about its cybersecurity practices, delaying its responses to the Executive Branch agencies during their mitigation monitoring, and as a result cannot be trusted to cooperate with the Executive Branch agencies, the Commission, and other U.S. government agencies. As discussed in the *Institution Order*, in a June 13, 2018 Letter, the Executive Branch agencies requested that CTA provide "*copies of China Telecom Americas' cybersecurity policies and procedures*{[
]}[479] When CTA provided responses to the Executive Branch agencies' questions on October 1, 2018, {[

[475] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111-13, April 4, 2019 Letter; *id.*, Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments; *id.*, at 19-20. We reject CTA's argument that it "did not commit to notify Team Telecom whenever someone outside the United States had access to its records; its sole obligation under the LOA was to give such notice if *a foreign government served legal process on CTA* – which has never happened." CTA June 8, 2020 Response, Exh. 16 at 38. We also reject CTA's argument that its "sole obligation" pursuant to the 2007 LOA is to "give notice if a foreign government served legal process on CTA," given that the 2007 LOA sets forth more than one requirement of CTA. *See* 2007 LOA; *see also infra* Section III.C.

[476] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111-13, April 4, 2019 Letter.

[477] *See supra* para. 107; Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621, EB-623, EB-628, December 6, 2018 Letter with Attachments.

[478] {[
]} *Id.*, Business Confidential Exh. 36 at EB-623; *see supra* para. 104 ({[ ]}).

[479] *See* CTA June 8, 2020 Response, Exh. 16 at 39-40, 68 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576) (emphasis added); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576, June 13, 2018 Letter. *See also Institution Order*, 35 FCC Rcd at 15030-31, para. 40.

[480] CTA June 8, 2020 Response, Exh. 16 at 26, 40 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 92 at EB-1983-85); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 92 at EB-1983-85, Oct. 1, 2018 Letter. *See also Institution Order*, 35 FCC Rcd at 15030-31, para. 40.

]}[483] On November 15, 2018, DOJ again sent an email to counsel, requesting a response no later than December 7, 2018.[484] On December 6, 2018, six months after the original request for copies of CTA's cybersecurity policies, CTA provided to DOJ {[ ]} Information Security Policy.[485] Furthermore, while CTA contends that the Information Security Policy was an effort to "memorialize numerous cybersecurity and privacy policies already implemented by CTA,"[486] despite being provided several opportunities, CTA did not provide documentation in this matter for the Commission to review these policies, to verify if and when they were implemented, and it is unclear whether all such policies identified by CTA even existed prior to {[ ]}[487]

112. CTA argues in its March 1, 2021 Reply that "the Commission[] [is] cherry-picking of the record relating to the communications between CTA and the Executive Branch,"[488] but it does not explain this argument with particularity. Additionally, CTA asserts that "the facts in the record demonstrat[e] that CTA has cooperated with and timely responded to inquiries from the Executive Branch agencies since at

[481] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586-87, November 26, 2018 Email. *See also Institution Order*, 35 FCC Rcd at 15030-31, para. 40.

[482] The agencies requested that CTA "'provide information management policies governing the sharing of U.S. customer information between [CTA] and its ultimate parent company, China Telecom Corporation. For example, how is personally identifiable information from U.S. customers treated and/or accessed?'" and "'the various business roles and responsibilities that are within the scope of CTA and those roles and responsibilities that reside with CTG and/or Chin[a] Telecom Corporation.'" CTA June 8, 2020 Response, Exh. 16 at 26-27, 40 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-587). *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586-87, November 26, 2018 Email ({

]}).

[483] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586, November 26, 2018 Email. *See also Institution Order*, 35 FCC Rcd at 15031, para. 40.

[484] Executive Branch Recommendation to Revoke and Terminate at 17, n.62 (citing, among other things, *id.*, Business Confidential Exh. 35 at EB-586 and noting "DOJ's fifth follow-up e-mail on Nov. 15, 2018"); CTA June 8, 2020 Response, Exh. 16 at 40 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586). *See also* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586, November 26, 2018 Email; *Institution Order*, 35 FCC Rcd at 15031, para. 40.

[485] CTA June 8, 2020 Response, Exh. 16 at 27, 41 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-654); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-654, December 6, 2018 Letter with Attachments. *See also Institution Order*, 35 FCC Rcd at 15031, para. 40. {[ ]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-654.

[486] CTA June 8, 2020, Response, Exh. 16 at 39.

[487] *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-590, December 6, 2018 Letter with Attachments ({[

]}). *See also Institution Order*, 35 FCC Rcd at 15031, para. 40.

[488] CTA Mar. 1, 2021 Reply at 31.

least 2007."[489] CTA states in its June 8, 2020 Response that its "current counsel has exchanged correspondence and participated in teleconferences or meetings with Team Telecom on at least 90 occasions since 2016."[490] However, CTA did not provide documentation of any such correspondence with the Executive Branch agencies and has cited solely to the correspondence filed on record by the Executive Branch agencies. We find no support in the record for CTA's claims, especially given the inconsistencies and omissions that are reflected in the record evidence concerning CTA's representations to the Executive Branch agencies. Moreover, CTA's characterization of a six-month response time to the Executive Branch agencies as "timely"[491] demonstrates CTA's lack of responsiveness to the Executive Branch agencies on critical national security and law enforcement concerns. CTA could have indicated to the Executive Branch agencies at the time of their inquiry that it {[

]}

113. We find unpersuasive CTA's justifications for its delay in responding to the Executive Branch agencies' inquiry about its cybersecurity policies and procedures. CTA argues in its June 8, 2020 Response that, "[h]ad Team Telecom desired CTA to respond to its request by a date certain, it could have done so in its initial request in June 2018, or in any of its subsequent correspondence over the next five months."[492] CTA further argues that "[t]he Commission (and the Executive Branch before it) discounts CTA's diligence and contends that CTA has not been consistent, transparent, and timely in its interactions with the Executive Branch."[493] {[

]}[495] In the June 13, 2018 Letter, the Executive Branch agencies expressly asked CTA to provide copies of its cybersecurity policies and procedures {[ ]}[496] The Executive Branch agencies reiterated the request for this information several times in their correspondences with CTA as of the June 13, 2018 Letter, {[

[489] *Id*. at 31-32 (citing CTA June 8, 2020 Response, Exh. 16 at 23-29, 64). CTA states in its June 8, 2020 Response, for example, that "CTA has communicated regularly and cooperatively with Team Telecom since at least 2007. . . . CTA has notified Team Telecom of certain events for which notice was required under the LOA on approximately five occasions." CTA June 8, 2020 Response, Exh. 16 at 64.

[490] CTA June 8, 2020 Response, Exh. 16 at 64.

[491] *Id*., Exh. 16 at 39.

[492] *Id*., Exh. 16 at 41.

[493] CTA Mar. 1, 2021 Reply at 31 (citing *Institution Order*, 35 FCC Rcd at 15029, para. 37).

[494] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576, June 13, 2018 Letter.

[495] CTA acknowledges in its June 8, 2020 Response that, when "members of Team Telecom met with CTA again to review its compliance with the 2007 LOA" in April 2018, "[f]or the first time, Team Telecom asked questions at that meeting about CTA's cybersecurity practices." CTA June 8, 2020 Response, Exh. 16 at 26.

[496] CTA June 8, 2020 Response, Exh. 16 at 39-40 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576, June 13, 2018 Letter.

[497] The record shows that DOJ sent three emails to counsel, on July 23, 2018, August 29, 2018, and September 17, 2018, asking about the status of the inquiry. Executive Branch Recommendation to Revoke and Terminate at 17 & n.62 (citing, among other things, *id.*, Business Confidential Exh. 33 at EB-578; *id.*, Business Confidential Exh. 34 at EB-581). {[

]} *Id.*, Business Confidential Exh. 34 at EB-582, Sept. 18, 2018 E-mail from Morgan Lewis to DOJ National Security

(continued….)

]}[498] Indeed, on November 15, 2018, DOJ again contacted counsel to request responses by December 7, 2018.[499]

114. The fact that CTA delayed its response to the Executive Branch agencies concerning compliance with the 2007 LOA is troubling, but even more significant is the record evidence indicating that CTA was not transparent and forthright to the Executive Branch agencies and the Commission about the reasons for its delay. CTA disputes the Executive Branch agencies' argument that it "is untrustworthy because it 'did not immediately disclose that it lacked a formal cybersecurity policy at the time,'" arguing instead that "the LOA does not require a formal cybersecurity policy" and that the agencies are "claiming that CTA 'did not immediately disclose' something that it was never asked for and had no obligation to have or to disclose."[500] The record shows that CTA provided no such argument or explanation to the Executive Branch agencies during the six months following the agencies' request for copies of CTA's cybersecurity policies and procedures,[501] until {[

]}[502] On September 17, 2018, DOJ sent an email to counsel, inquiring again about the status of the requested information, {[

]}

115. Significantly, CTA's attempt to withhold information from the Executive Branch agencies by {[

(Continued from previous page)
Division (Sept. 18, 2018 Email); *id.*, Business Confidential Exh. 33 at EB-578, Aug. 30, 2018 E-mail from Morgan Lewis to DOJ National Security Division.

[498] *Id*., Business Confidential Exh. 35 at EB-587, November 26, 2018 Email.

[499] Executive Branch Recommendation to Revoke and Terminate at 17, n.62 (citing, among other things, *id.*, Business Confidential Exh. 35 at EB-586 and noting "DOJ's fifth follow-up e-mail on Nov. 15, 2018"); CTA June 8, 2020 Response, Exh. 16 at 40 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586). *See also* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586, November 26, 2018 Email; *Institution Order*, 35 FCC Rcd at 15031, para. 40.

[500] CTA June 8, 2020 Response, Exh. 16 at 39 (quoting Executive Branch Recommendation to Revoke and Terminate at 17).

[501] Executive Branch Recommendation to Revoke and Terminate at 17 (citing *id.*, Business Confidential Exh. 32 at EB-576).

[502] *Id*., Business Confidential Exh. 36 at EB-589-593, December 6, 2018 Letter with Attachments.

[503] *Id*. at 17, n.62; CTA June 8, 2020 Response, Exh. 16 at 40 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-586); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 34 at EB-581, September 18, 2018 Email.

[504] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-590, December 6, 2018 Letter with Attachments.

]}[509] In view of such conduct, and considering the language that was redacted, it is apparent that CTA cannot be trusted to comply with its obligations under the 2007 LOA, irrespective of whether it is responding to the Executive Branch agencies' compliance monitoring at a given time. CTA's attempts to justify its conduct rather than admit it erred further add to our concerns that CTA cannot be trusted to be cooperative, transparent, and forthright with the Commission and other U.S. government agencies.

116. Moreover, we find based on the record that CTA cannot be relied upon to comply with the Commission's rules and procedures. As we discuss further in Section III.C, the record demonstrates that CTA did not notify the Executive Branch agencies of its applications for ISPC assignments, as mandated by the 2007 LOA, and compliance with which is an express condition of CTA's international section 214 authorizations.[510] Further, CTA disregarded its responsibilities to the Commission as a holder of ISPCs.[511] On November 18, 2020, based on information that CTA filed in response to the *Order to Show Cause*, the International Bureau found that CTA was not in compliance with the conditions of its

[505] Executive Branch Response at 7 (citing Executive Branch Recommendation to Revoke and Terminate at 18 and *id.*, Business Confidential Exh. 37 at EB-655); *see also* Executive Branch Recommendation to Revoke and Terminate at 56 (quoting *id.*, Business Confidential Exh. 37 at EB-655; CTA June 8, 2020 Response, Exh. 16 at 22, n.40.

[506] CTA June 8, 2020 Response, Exh. 16 at 22, n.40. CTA makes no mention of the fact that it had {[ ]} *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 37 at EB-655-656, January 24, 2019 e-mail from Morgan Lewis to DOJ National Security Division (January 24, 2019 Email).

[507] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 37 at EB-655, January 24, 2019 Email. {[ ]} *Id.*

[508] {[ ]} *Id*., Business Confidential Exh. 36 at EB-630, December 6, 2018 Letter with Attachments.

[509] *Id*., Business Confidential Exh. 37 at EB-655, January 24, 2019 Email.

[510] *See infra* Section III.C.; *Institution Order*, 35 FCC Rcd at 15032, para. 42; CTA June 8, 2020 Response, Exh. 16 at 6, 69-70; 2007 LOA at 2-3 ("The Company agrees that it will notify the FBI, DOJ and DHS . . . if it undertakes any actions that require notice to or application to the FCC.").

[511] *Institution Order*, 35 FCC Rcd at 15032, para. 42.

provisional ISPC assignments, and reclaimed the three ISPCs.[512] Specifically, CTA did not comply with the Commission's ISPC requirements when it failed to notify the Commission that ISPC {[ ]} has not been in use since {[ ]} was "not ultimately configured for use."[513] CTA had prior knowledge of these requirements and even made certifications in its ISPC applications.[514] CTA's failure to comply with a condition of the 2007 LOA and the Commission's own requirements affirms our concerns regarding CTA's lack of candor, trustworthiness, and reliability.

117. Based on the overwhelming record evidence, we find that the Commission, Executive Branch agencies, and other U.S. government agencies cannot trust CTA especially in light of the serious national security and law enforcement concerns associated with CTA's vulnerability to exploitation, influence, and control by the Chinese government.[515] The trust, transparency, and reliability that are essential to the effectiveness of a mitigation agreement and to an authorization holder's ability to comply with the Commission's statutory authority and implementing rules are simply not present with CTA. Independent of our concerns above, we separately revoke CTA's section 214 authority based on CTA's past conduct and representations to the Commission and other U.S. government agencies to protect the national security and law enforcement interests of the United States.

C. Termination of International Section 214 Authorizations

118. Separate and apart from our findings concerning revocation of CTA's section 214 authority, we terminate CTA's international section 214 authorizations based on CTA's willful violation of two of the five provisions of the 2007 LOA, compliance with which is an express condition of CTA's international section 214 authorizations.[516] Pursuant to section 214(c) of the Act, the Commission "may attach to the issuance of the certificate such terms and conditions as in its judgment the public convenience and necessity may require."[517] CTA's two international section 214 authorizations, ITC-214-20010613-00346 and ITC-214-20020716-00371, are expressly conditioned upon it abiding by the

[512] *Id.*; *see* ISPC Reclamation Letter.

[513] *Institution Order*, 35 FCC Rcd at 15032, para. 42; ISPC Reclamation Letter at 1-2, 4; CTA June 8, 2020 Response, Exh. 9 at 2; *see* Letter from Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP, to Marlene H. Dortch, Secretary, FCC (Dec. 2, 2020) (on file in File Nos. SPC-NEW-20030314-00014, SPC-NEW-20100314-00006, SPC-NEW-20100326-00007) (Response to ISPC Reclamation Letter). CTA does not accept the view that it has been warehousing these ISPCs or is acting or has acted inappropriately, but "is willing to relinquish its ISPCs to ensure that there is no constraint on such numbering resources." Response to ISPC Reclamation Letter at 2.

[514] *Institution Order*, 35 FCC Rcd at 15032, para. 42; ISPC Reclamation Letter at 1-4 (stating, for example, "[p]ursuant to ITU-T Recommendation Q.708, the Commission required [CTA] to make several certifications in its applications for the ISPCs," and "[i]n its letters provisionally assigning the ISPCs to [CTA], the International Bureau reiterated the certifications.").

[515] *See supra* Section III.B.2.

[516] *2007 Pro Forma Grant Public Notice*, 22 FCC Rcd at 15268 ("[W]e condition grant of this pro forma transfer of control on China Telecom (USA) Corporation abiding by the commitments and undertakings contained in its July 17, 2007 [LOA] . . . ."). *See Institution Order*, 35 FCC Rcd at 15033-34, para. 47 (citing *P & R Temmer v. FCC*, 743 F.2d 918 (D.C. Cir. 1984); *Atlantic Richfield Co. v. United States*, 774 F.2d 1193 (D.C. Cir. 1985); *Morris Communications, Inc. v. FCC*, 566 F.3d 184 (D.C. Cir. 2009) (automatic termination for non-payment did not violate administrative due process because in such situation "the licenses themselves . . . lapsed); *Alpine PCS, Inc. et al.; Requests for Waiver of the Installment Payment Rules and Reinstatement of Licenses*, Memorandum Opinion and Order, 25 FCC Rcd 469 (2010), *aff'd*, 404 Fed. Appx. 508 (D.C. Cir. 2010) (*Alpine PCS*) (provision for automatic cancellation did not trigger section 312(a) revocation procedures)).

[517] 47 U.S.C. § 214(c).

commitments and undertakings contained in its 2007 LOA.[518] The 2007 LOA provides that, "in the event the commitments set forth in this letter are breached, in addition to any other remedy available at law or equity, the DOJ, FBI, or DHS may request that the FCC modify, condition, revoke, cancel, or render null and void any relevant license, permit, or other authorization granted by the FCC to the Company or any successor-in-interest to the Company."[519]

119. Based on the record evidence, we find that CTA willfully violated two of the five provisions of the 2007 LOA by failing to: (1) "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA];"[520] and (2) "notify the FBI, DOJ and DHS if there are material changes in any of the facts as represented in [the 2007 LOA] or if it undertakes any actions that require notice to or application to the FCC."[521] Although CTA had "an opportunity to either explain or rectify" any breach of the terms of the 2007 LOA,[522] it has failed to do so. Because compliance with the commitments contained in the 2007 LOA is an express condition of its international section 214 authorizations, CTA's failure to comply with the commitments accordingly warrants termination of such authorizations.[523]

120. *Failure to Take All Practicable Measures to Prevent Unauthorized Access to U.S. Records*. We find that CTA failed to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]."[524] The Commission and the Executive

[518] *2007 Pro Forma Grant Public Notice*, 22 FCC Rcd at 15268 ("[W]e condition grant of this pro forma transfer of control on China Telecom (USA) Corporation abiding by the commitments and undertakings contained in its July 17, 2007 [LOA] . . . ."). The 2007 LOA contains five key provisions requiring CTA to (1) "make . . . U.S. Records available in the United States in response to lawful U.S. process"; (2) "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]"; (3) "not, directly or indirectly, disclose or permit disclosure of or access to U.S. Records, domestic communications or to any information (including the content of communications) pertaining to a wiretap order, pen/trap order, subpoena, or other lawful demand by a U.S. law enforcement agency for U.S. Records, to any person if the purpose of such disclosure or access is to respond to the legal process or request on behalf of a non-U.S. government without first satisfying all pertinent requirements of U.S. law and obtaining the express written consent of the FBI, DOJ and DHS or the authorization of a court of competent jurisdiction in the United States"; (4) "maintain one or more points of contact within the United States with the authority and responsibility for accepting and overseeing compliance with a wiretap order, pen/trap order, subpoena or other lawful demand by U.S. law enforcement authorities for the content of communications or U.S. Records"; and (5) "notify the FBI, DOJ and DHS if there are material changes in any of the facts as represented in [the 2007 LOA] or if [CTA] undertakes any actions that require notice to or application to the FCC." 2007 LOA at 2-3. The 2007 LOA defines U.S. Records as "all customer billing records, subscriber information, and any other related information used, processed, or maintained in the ordinary course of business relating to communications services offered to U.S. persons." *Id.* at 2.

[519] 2007 LOA at 3.

[520] Executive Branch Recommendation to Revoke and Terminate at 53; 2007 LOA at 2; *see also* Executive Branch Response at 7, 14.

[521] Executive Branch Recommendation to Revoke and Terminate at 53; 2007 LOA at 2-3; *see also* Executive Branch Response at 7, 14.

[522] 2007 LOA at 3.

[523] *See P & R Temmer v. FCC*, 743 F.2d 918 (D.C. Cir. 1984); *Atlantic Richfield Co. v. United States*, 774 F.2d 1193 (D.C. Cir. 1985); *see also Morris Communications, Inc. v. FCC*, 566 F.3d 184 (D.C. Cir. 2009) (automatic termination for non-payment did not violate administrative due process because in such situation "the licenses themselves . . . lapsed); *Alpine PCS* (provision for automatic cancellation did not trigger section 312(a) revocation procedures).

[524] 2007 LOA at 2.

Branch agencies have a strong interest in ensuring CTA's compliance with this obligation because, as stated above, like all telecommunications carriers with access to PII,[525] CTA has a statutory responsibility to ensure the protection of this sensitive information.[526] In particular, CPNI includes some of the most sensitive personal information that carriers and providers have about their customers as a result of their business relationship, much of which is highly sensitive.[527] The Commission has adopted rules to ensure that CPNI is adequately protected from unauthorized access, use, or disclosure.[528] Furthermore, as a condition of its international section 214 authorizations, CTA was required to implement "all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records . . . ."[529]

121. *First*, we find that CTA failed to fully identify or explain the steps it has taken since 2007 to comply with the requirement to "take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]." The "measures" identified by CTA in the in the record do not amount to taking "all practicable measures" to prevent unauthorized access to communications or U.S. customer records {[ ]} Although it was afforded several opportunities to respond to the Commission, CTA only provided bare statements about how it complied with this provision of the 2007 LOA. CTA included a list of policies "concerning information security" but did not explain with particularity how these policies protect the U.S. records.[530] Importantly, CTA did not provide copies of its policies or any evidence to the Commission to demonstrate when the policies were implemented and, in some circumstances, whether such policies even existed. Indeed, CTA itself solely relied on and cited to instances where {[ ]}[531]

122. Based on the record, the Executive Branch agencies sent CTA a letter on June 13, 2018 requesting "'copies of China Telecom Americas' cybersecurity policies and procedures'"[532] as well as responses to specific questions, including what tools CTA uses "to defend production networks, and/or customer networks, from harmful cyber-attacks" and whether "People's Republic of China public security agencies [have] engaged in inspections of, or required information regarding, [CTA] operations, including any virtual private networks utilized as part of such operations[.]"[533] CTA did not provide a copy of its

[525] *See TerraCom NAL*, 29 FCC Rcd at 13331, para. 17 (stating that "[i]n general, PII is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context").

[526] 47 U.S.C. § 222 (ensuring the privacy of customer information); *id* at § 222(a) ("[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.").

[527] *CPNI Order*, 22 FCC Rcd at 6931, para. 5.

[528] 47 CFR §§ 64.2001-.2011.

[529] 2007 LOA at 2.

[530] CTA June 8, 2020 Response, Exh. 16 at 67.

[531] *See, e.g.*, *id*., Exh. 16 at 22 n.40, 27 nn.52-53, 28 n.57, 40 n.82, 41 n.89 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exhs. 36, 103, 92, 37).

[532] *See id*., Exh. 16 at 39-40, 68 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576.

[533] *See* CTA June 8, 2020 Response, Exh. 16 at 26 (referring to Executive Branch Recommendation to Revoke and Terminate, Exh. 32 at EB-577); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576-77, June 13, 2018 Letter; *see also id.*, Business Confidential Exh. 34 at EB-583, September 18, 2018 Email. *See supra* para. 111.

cybersecurity policies and procedures to the Executive Branch agencies until December 6, 2018.[534] At that time, CTA provided the Executive Branch agencies with copies of {[ ]} Information Security Policy {[ ]} and the U.S. Records Security Agreement between CTA and CTCL, {[ ]}[535] When asked by the Executive Branch agencies {[

]}[536]

123. {[

]}[539]

[534] CTA June 8. 2020 Response, Exh. 16 at 27, 39-41 (citing, e.g., Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exhibit 36 at EB-589-654); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-90, December 6, 2018 Letter with Attachments.

[535] CTA June 8. 2020 Response, Exh. 16 at 27, 41 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exhibit 36 at EB-589-654); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-590-654, December 6, 2018 Letter with Attachments. CTA {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-590-654. Significantly, {[ ]} CTA had improperly redacted the 2018 U.S. Records Security Agreement to omit {

]} Executive Branch Response at 7 & n.28 (citing Executive Branch Recommendation to Revoke and Terminate at 18, n.65 (citing *id.*, Business Confidential Exh. 37 at EB-655)). *See also* Executive Branch Recommendation to Revoke and Terminate at 18, 56 (quoting *id*., Business Confidential Exh. 37 at EB-655).

[536] CTA June 8, 2020 Response, Exh. 16 at 66 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 37 at EB-655); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 37 at EB-655-56, January 24, 2019 Email.

[537] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 102 at EB-2103, March 21, 2019 Letter; *see also id.*, Business Confidential Exh. 96 at EB-2000, March 21, 2019 Letter.

[538] *Id*., Business Confidential Exh. 103 at EB-2108, April 4, 2019 Letter.

[539] *Id*., Business Confidential Exh. 119 at EB-2745, May 29, 2019 Letter from DOJ National Security Division to Morgan Lewis (May 29, 2019 Letter); *see also Institution Order*, 35 FCC Rcd at 15034, para. 51, n.194 (quoting Executive Branch Recommendation to Revoke and Terminate at 54). The Executive Branch agencies state that {[

]} Executive Branch Recommendation to Revoke and Terminate at 54. The Executive Branch agencies added that {[

]} Executive (continued….)

124. In the *Order to Show Cause*, the Bureaus directed CTA to submit "a detailed response to the allegations raised in the [Executive Branch Recommendation to Revoke and Terminate],"[540] which include the Executive Branch agencies' allegation that CTA "failed to take 'all practicable measures' to prevent unauthorized access to U.S. records" in breach of the 2007 LOA.[541] In its June 8, 2020 Response, CTA contends that the 2007 LOA "does not require CTA to implement a single, comprehensive cybersecurity policy" and that CTA had "met its commitment in the LOA by consistently and continuously implementing and updating a variety of measures to prevent unauthorized access to or disclosure of U.S. Records that CTA actually collects and maintains in the course of provisioning and billing services to customers."[542] CTA also asserts that "the LOA left it to CTA to implement 'practicable' measures appropriate to its network and services" and that "[b]ecause the LOA is silent on specific requirements regarding CTA's information security policies, the fact that CTA fulfilled its obligations in a different manner than Team Telecom might have preferred cannot constitute a breach of the LOA."[543]

125. In its June 8, 2020 Response to the *Order to Show Cause*, CTA states that its {[

]} and that "[b]efore completing Version 1.0 in December 2018, CTA followed a number of its own written policies concerning information security, including {[

]}[544] CTA states that it "also has Physical Access Guidelines and Policies ('Physical Access Policies') that outline strict controls for access to CTA's POPs and data centers."[545] However, as discussed below, CTA did not provide documentation for the Commission to review these policies. Moreover, after examining CTA's communications with the Executive Branch agencies,{[

(Continued from previous page)
Branch Recommendation to Revoke and Terminate at 54-55; *see Institution Order*, 35 FCC Rcd at 15034, para. 51, n.194.

[540] *Order to Show Cause*, 35 FCC Rcd at 3719, para. 12.

[541] Executive Branch Recommendation to Revoke and Terminate at 54.

[542] CTA June 8, 2020 Response, Exh. 16 at 66.

[543] *Id*.; *see also Institution Order*, 35 FCC Rcd at 15035, para. 52, n.199.

[544] CTA June 8, 2020 Response, Exh. 16 at 67 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-590; *id.*, Exh. 103 at EB-2113).

[545] *Id*.

[546] {[

]} *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2108, April 4, 2019 Letter. In its June 8, 2020 Response to the *Order to Show Cause*, CTA cites to {[

]} CTA June 8, 2020 Response, Exh. 16 at 67, n.165 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at 2113).

]}[547]

126. Importantly, despite the Commission providing CTA with several opportunities to submit evidence of compliance with this provision of the 2007 LOA,[548] CTA again failed to provide clear explanations, copies of the policies, or other documentation for the Commission to verify if and when any such policies were implemented. As the Commission stated in the *Institution Order*, "[t]hough the 2007 LOA may not specify the exact measures for a cybersecurity policy (or that it must be in writing), [the Commission has] no evidence of what measures (if any) [CTA] adopted to comply with the requirements of the 2007 LOA,"[549] or when any measures were implemented.[550] Specifically, the Commission indicated in the *Institution Order* that CTA failed to "provide documentation for the Commission to review the policies, to verify if and when they were implemented, and it is unclear whether such policies even existed prior to {[ ]}"[551] The Commission noted that {[

]}[552] Nevertheless, in its March 1, 2021 Reply, CTA did not proffer any other evidence or any additional arguments as to exactly what "practicable measures" were in fact implemented to comply with the 2007 LOA.

127. Based on the record, CTA failed to provide *any* additional persuasive record support to "dispute[] the assertion that [it] failed to take 'all practicable measures' to prevent unauthorized access to U.S. records."[553] Based on CTA's own admission, it appears that the first policy concerning information security {[ ]}[554] The Executive Branch

[547] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2113, April 4, 2019 Letter.

[548] 2007 LOA at 2 ("take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth in [the 2007 LOA]").

[549] *Institution Order*, 35 FCC Rcd at 15035-36, para. 52.

[550] *Id.* at 15036, para. 52.

[551] *Id*.

[552] *Id.* at 15036, n.205 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-91, EB-642-654; CTA June 8, 2020 Response, Exh. 16 at 40-41). *See* CTA June 8, 2020, Exh. 16 at 40-41 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-585) (citing DOJ email request, "[p]lease explain the CALEA compliance process at [CTA] and CTExcel. Please list other companies that are used by CTA and CTExcel to fulfil all government legal service."); *see also* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-585, November 26, 2018 Email.

[553] CTA Mar. 1, 2021 Reply at 31 (citing CTA June 8, 2020 Response, Exh. 16 at 4, 6, 39-42, 65-69; *Institution Order*, 35 FCC Rcd at 15035-36, para. 52).

[554] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2113, April 4, 2019 Letter; CTA June 8, 2020 Response, Exh. 16 at 67. {[

(continued….)

agencies provided in their Recommendation two copies of an undated CPNI Policy that CTA submitted to the Commission with its CPNI Certifications in 2018 and 2019, {[ ]}[555] Although CTA argues that the 2007 LOA does not "specify the provisions or issues that should be included, impose cybersecurity standards CTA must follow, or set a timeline for when such any specific policy or standard must be implemented,"[556] {[ ]} fails to fulfill the requirement that CTA take "all practicable measures" to protect sensitive communications and U.S. records. {[

]}[557]

128. The record includes a copy of CTA's {[

]}[558] However, we do not find CTA's {[

(Continued from previous page)

]}

[555] Executive Branch Recommendation to Revoke and Terminate, Exh. 94 at EB-1990-94, China Telecom Americas, CPNI Certification (Mar. 1, 2018), https://ecfsapi.fcc.gov/file/102283055404711/CHINA_TELECOM_AMERICAS_CPNI_CERTIFICATION_03_01_2018_SIGNED.PDF; *id.*, Exh. 95 at EB-1995-99, China Telecom Americas, CPNI Certification (Feb. 28, 2019), https://ecfsapi.fcc.gov/file/10228382226430/CHINA_TELECOM_AMERICAS_CPNI_CERTIFICATION_02_28_2019.pdf; *id.*, Business Confidential Exh. 103 at EB-2113, April 4, 2019 Letter; CTA June 8, 2020 Response, Exh. 16 at 67.

[556] CTA June 8, 2020 Response, Exh. 16 at 66.

[557] *See, e.g.*, Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2113, April 4, 2019 Letter; CTA June 8, 2020 Response, Exh. 16 at 67. {[

]} *See id.*, Business Confidential Exh. 103 at EB-2113; CTA June 8, 2020 Response, Exh. 16 at 67.

[558] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36, at EB-589-591, EB-642-654, December 6, 2018 Letter with Attachments; *see also Institution Order*, 35 FCC Rcd at 15036, para. 52 & n.205.

]} determinative of CTA's compliance with the requirement to take "all practicable measures" to prevent unauthorized access to communications and U.S. records. This policy provides details concerning {[

]}[559] but CTA does not describe how its {[ ]} protects communications and U.S. records.[560] The Executive Branch agencies also included in their Recommendation a copy of CTA's 2018 U.S. Records Security Agreement.[561] CTA asserts that it "entered into an arms-length Records Security Agreement with its parent company expressly for, among other things, the purpose of ensuring compliance with the LOA,"[562] but we do not view this Agreement as a "practicable measure[]," as we discuss in greater detail below.

129. In the absence of any such additional evidence from CTA, we find that based on the record, CTA did not implement a formal, comprehensive cybersecurity policy until the Executive Branch agencies made this inquiry in 2018.[563] This finding is supported by the evidence from the Executive Branch agencies indicating that {[

]} request for "copies of China Telecom Americas' cybersecurity policies and procedures" in June 2018.[564] CTA also fails to provide any additional information as to the status of {[

]}

[559] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36, at EB-591, December 6, 2018 Letter with Attachments.

[560] *Id*., Business Confidential Exh. 36, at EB-642-650, December 6, 2018 Letter with Attachments.

[561] CTA June 8, 2020 Response, Exh. 16 at 22, n.40 (citing Executive Branch Recommendation, Business Confidential Exh. 36 at EB-590 and noting "introducing the U.S. Records Security Agreement"); *id.*, Exh. 16 at 52, n.118; Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36, at EB-589-590, EB-621-637, December 6, 2018 Letter with Attachments.

[562] CTA June 8, 2020 Response, Exh. 16 at 52.

[563] CTA June 8, 2020 Response, Exh. 16 at 65 (quoting Executive Branch Recommendation to Revoke and Terminate at 54); *see also Institution Order*, 35 FCC Rcd at 15034, para. 51. In the *Institution Order*, the Commission pointed to a {

]} CTA "provided {[ ]} Information Security Policy to DOJ on December 6, 2018, approximately six months after the Executive Branch agencies requested copies of [CTA's] cybersecurity policies and procedures in their June 13, 2018 letter." *See* CTA June 8, 2020 Response, Exh. 16 at 27, 41 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-654). *See also Institution Order*, 35 FCC Rcd at 15034-35, n.195 (citations omitted).

[564] *See* CTA June 8, 2020 Response, Exh. 16 at 39-40, 68 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576, June 13, 2018 Letter. {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-586-87, EB-590, EB-630, December 6, 2018 Letter with Attachments.

130. *Second*, even if we were to accept CTA's suggestion that it had in the past or may have existing "security policies and procedures" to protect U.S. records,[565] CTA has provided no evidence that it enforces or abides by any such policies despite the serious concerns raised by the record that CTA is placing U.S. records at risk for unauthorized access and disclosure.[566] {[

]}[567] CTA provided the Executive Branch agencies with a copy of its 2018 U.S. Records Security Agreement with its direct parent, CTCL, on December 6, 2018.[568] {[

]} request for "copies of China Telecom Americas' cybersecurity policies and procedures,"[569] {[

]}[570] According to CTA, "the U.S. Records Security Agreement . . . governs access to U.S. Records, including by CTA's non-U.S. affiliates."[571] {[

]}[572] The record shows, however, that when requested by the Executive Branch agencies in March 2019 to "provide all access logs kept by [CTA] regarding non-U.S. affiliate access to U.S. records" {[

[565] CTA June 8, 2020 Response, Exh. 16 at 69 (stating, "[t]he fact that several pre-existing security policies and procedures were not consolidated into a single, written document until December 2018 does not mean that the policies did not exist, that CTA failed to take measures to protect its customer information, or that it breached its obligations under the LOA.").

[566] *Institution Order*, 35 FCC Rcd at 15034-38, paras. 50-54.

[567] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at 586-587, November 26, 2018 Email; *id.*, Business Confidential Exh. 36 at EB-590, EB-620-37, December 6, 2018 Letter with Attachments.

[568] CTA June 8, 2020 Response, Exh. 16 at 22, 27-28; Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at 586-87, EB-590, December 6, 2018 Letter with Attachments.

[569] *See* CTA June 8, 2020 Response, Exh. 16 at 39-40 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576); *see* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 32 at EB-576, June 13, 2018 Letter.

[570] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2108, April 4, 2019 Letter.

[571] CTA June 8, 2020 Response, Exh. 16 at 22.

[572] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments.

[573] CTA June 8, 2020 Response, Exh. 16 at 38 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 96 at EB-2003). *See* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 96 at EB-2000, EB-2003, March 21, 2019 Letter; *id.*, Business Confidential Exh. 102 at EB-2103, EB-2106, March 21, 2019 Letter.

]}[574]

131. In its June 8, 2020 Response to the *Order to Show Cause*, CTA contends that the Executive Branch agencies characterize CTA's failure to provide database access logs to Team Telecom "[as] a violation of CTA's obligations under the inter-company U.S. Records Security Agreement, not a violation of the LOA or of any commitment made to Team Telecom" and that the Executive Branch Recommendation to Revoke and Terminate does not allege "any misconduct that is cognizable by the Commission[.]"[575] We disagree with CTA's argument that its failure to provide the access logs has no bearing on whether or not CTA breached the 2007 LOA.

132. Even if we were to accept CTA's argument that enforcement of the terms of the 2018 U.S. Records Security Agreement was intended to be a key part of CTA's measures for preventing unauthorized access to U.S. records, the record shows that CTA did not adhere to that Agreement. Indeed, CTA represents to the Commission, more than once, that the 2018 U.S. Records Security Agreement was entered into "expressly for, among other things, the purpose of ensuring compliance with the LOA."[576] By failing to maintain these access logs, CTA failed to enforce the "security policies and procedures" that it purportedly had in place, demonstrating that these policies and procedures do not amount to "practicable measures" that would protect U.S. records and communications. Importantly, CTA does not address the fact that {[

]} CTA has offered no evidence that the 2018 U.S. Records Security Agreement, or any of its "security policies and procedures," rise to the level of "practicable measures" that would prevent unauthorized access to U.S. records. CTA's admitted failure to comply with its own policy aimed at protecting U.S. records does not amount to "practicable measures" to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records.

133. *Third*, we find that CTA's practice of knowingly {[
]} without honoring its commitment to disclose this fact to the Executive Branch agencies, {[
]} amounts to a willful violation of the requirement to take "all practicable measures" to

---

[574] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2112-13, April 4, 2019 Letter.

[575] CTA June 8, 2020 Response, Exh. 16 at 37-38. In its June 8, 2020 Response to the *Order to Show Cause*, CTA did not address the fact that the 2018 U.S. Records Security Agreement {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments. Instead, CTA states that it had indicated to the Executive Branch agencies that "'[a]ccessing these logs would require significant manpower and time, as it involves machine-level information located on multiple servers.' CTA's response did not 'decline' to obtain the access logs maintained by its affiliates, or state that it 'could not' provide them." CTA June 8, 2020 Response, Exh. 16 at 38 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2113).

[576] CTA June 8, 2020 Response, Exh. 16 at 52; *see also* CTA Mar. 1, 2021 Reply at 32 ("And instead of providing any evidence showing that CTA is vulnerable to 'foreign government' requests, the only example provided in support of the Executive Branch's allegation is based on a (mis)interpretation of a Records Security Agreement between CTA and its parent company, *entered for the purpose of ensuring compliance with the LOA*." (emphasis added)).

[577] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2111-2113, April 4, 2019 Letter; *see supra* note 455.

prevent unauthorized access to U.S. records.[578] CTA provides no additional evidence or arguments concerning the discrepancy between CTA's {[

]} inform Team Telecom if it intends to store any U.S. business records outside the United States prior to doing so,"[579] and {[

]}[580] As the Commission stated in the *Institution Order*, {[

]}[581] Further, "[t]he answers also provide context as to how [CTA] would 'take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. Records, in violation of any U.S. Federal, state, or local laws or of the commitments set forth [in the 2007 LOA].'"[582] {[

]}[584] We find that, taking into consideration the totality of the evidence in the record and the absence of any evidence to the contrary, CTA failed to take all practicable measures[585] to prevent unauthorized access to its U.S. Records as required by the 2007 LOA, and it is in breach of its mitigation agreement with the

[578] *See supra* paras. 107-10; Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15, May 11, 2007 Response; *id.*, Business Confidential Exh. 125 at EB-2783, January 11, 2016 Letter; *id.*, Business Confidential Exh. 103 at EB-2111-12, April 4, 2019 Letter; *see* CTA June 8, 2020 Response, Exh. 16 at 28-29. *See also Institution Order*, 35 FCC Rcd at 15029-30, 15037-38, paras. 38-39, 54.

[579] *See* CTA June 8, 2020 Response, Exh. 16 at 38 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15, May 11, 2007 Response; *see supra* Section III.B.3.; *see also Institution Order*, 35 FCC Rcd at 15036-38, paras. 53-54.

[580] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624, December 6, 2018 Letter with Attachments (emphasis added); *see also Institution Order*, 35 FCC Rcd at 15037, para. 54. The Commission has also expressed concern with CTA's {[

]} *Institution Order*, 35 FCC Rcd at 15037-38, n.214 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-624). CTA also asserts that "[e]lectronic records can be 'kept' at one location and simultaneously be 'available' in other locations," but this interpretation does not explain why CTA did not notify the Executive Branch agencies before making these records available outside of the United States. CTA June 8, 2020 Response, Exh. 16 at 21, 22.

[581] *Institution Order*, 35 FCC Rcd at 15038, para. 54 ({[

]}).

[582] *Id*. (quoting 2007 LOA at 2).

[583] *Id.*

[584] Executive Branch Recommendation to Revoke and Terminate at 21; *Institution Order*, 35 FCC Rcd at 15037-38, para 54.

[585] The Commission stated in the *Institution Order* that {[

]} *Institution Order*, 35 FCC Rcd at 15038, para. 54.

Executive Branch agencies. Given the absence of record evidence to support CTA's assertions, we also find that the written record presents no substantial and material questions of fact with respect to this matter.

134. *Failure to Notify Executive Branch Agencies of Applications for ISPCs*. The record evidence clearly shows that CTA breached the 2007 LOA provision requiring that it "notify the FBI, DOJ and DHS if there are material changes in any of the facts as represented in [the 2007 LOA] or if it undertakes any actions that require notice to or application to the FCC."[586] In particular, we find that the record supports the Executive Branch agencies' contentions that "[CTA] failed to inform the FBI, DOJ and DHS at least twice in 2010 when it filed notices to the FCC."[587] Specifically, the Executive Branch agencies indicate CTA filed two separate applications for ISPCs,[588] and {[

]}[589] CTA does not dispute that it did not notify the Executive Branch agencies of its applications for the ISPCs. Rather, in its responses to both the *Order to Show Cause* and the *Institution Order*, CTA insists that ISPC applications are "trivial, ministerial filings" that do not require prior notification to the Executive Branch agencies.[590] Additionally, CTA contends that "there is clear disagreement between CTA, the Executive Branch, and the Commission as to whether the LOA requires CTA to notify the Executive Branch of 'substantive applications,' rather than 'ministerial requests' such as the assignment of numbering resources."[591] We reject these arguments for the reasons below.

135. *First*, we again reject CTA's argument that requests for assignments of numbering resources are "ministerial."[592] As the Commission noted in the *Institution Order*, "ISPCs are a scarce resource that are used by international Signaling System 7 (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. . . . Despite [CTA's] claims, the assignment of international SS7 routing addresses remains a non-trivial resource regardless of whether, or to what extent, [CTA] chooses to deploy SS7."[593] Further, the Commission noted in the

---

[586] 2007 LOA at 2-3; *see Institution Order*, 35 FCC Rcd at 15038, para. 55.

[587] Executive Branch Recommendation to Revoke and Terminate at 55 & n.199.

[588] *Id*. at Business Confidential Exh. 96, EB-2000, March 21, 2019 Letter; *id*., Business Confidential Exh. 102, EB-2103, March 21, 2019 Letter; *see also id*., Business Confidential Exh. 103 at EB-2108-09, April 4, 2019 Letter; File Nos. SPC-NEW-29199326-00007 and SPC-NEW-20100314-00006.

[589] *Institution Order*, 35 FCC Rcd at 15038-39, para. 55 (quoting Executive Branch Recommendation to Revoke and Terminate at 55). {[

]} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 119 at EB-2746, May 29, 2019 Letter.

[590] CTA June 8, 2020 Response, Exh. 16 at 70; *see* CTA Mar. 1, 2021 Reply at 31 (referring to ISPC assignment requests as "'ministerial requests'").

[591] CTA Mar. 1, 2021 Reply at 31; *see* CTA June 8, 2020 Response, Exh. 16 at 70 ("If the LOA only required CTA to advise Team Telecom of 'material' changes in facts, it is reasonable to construe the requirement to advise of an 'application' or 'notice' to be limited to material FCC filings."). The Executive Branch agencies make no such distinction concerning the materiality of ISPC applications in their Recommendation; rather, they refer to the ISPC applications as "notices" and {[

]} Executive Branch Recommendation to Revoke and Terminate at 55; *id*., Business Confidential Exh. 102 at EB-2103, March 21, 2019 Letter.

[592] *See Institution Order*, 35 FCC Rcd at 15040, para. 58.

[593] *Id*.

Institution Order that "the International Bureau recently reclaimed [CTA's] three ISPCs as '[CTA] is not in compliance with the conditions of its provisional ISPC assignments.' Reclamation of [CTA's] IPSCs was due to [CTA's] disregard of the Commission's rules and requirements and further undermines the suggestion that an application for an ISPC is purely a ministerial or trivial filing."[594]

136. *Second*, CTA's attempts to undermine the importance of ISPCs to justify its failure to report its ISPC applications to the Executive Branch agencies fails upon a plain reading of the 2007 LOA. CTA argued {[

]}[595] According to CTA, {[

]}[596] As the Commission noted in the *Institution Order*, "[b]y its terms, the 2007 LOA requires that [CTA] 'will notify the FBI, DOJ and DHS if there are material changes in any of the facts as represented in [the 2007 LOA] *or* if it undertakes any actions that require notice to or application to the FCC.' In this case, the record evidence shows that [CTA] filed applications for ISPCs with the Commission without prior notification to the Executive Branch agencies."[597] There is simply no evidence in the record that the 2007 LOA required notification of only "'substantive applications,'" as CTA claims.[598] The written record presents no substantial and material questions of fact with respect to this matter as CTA freely admits that it failed to notify the Executive Branch agencies of its 2010 ISPC applications, and this clearly constitutes a willful breach of the plain language of the 2007 LOA.

137. We find that although CTA had "an opportunity to either explain or rectify" any breach of the terms of the 2007 LOA,[599] it has failed to do so. CTA argued that {[

]}[600] We view CTA's response to the Executive Branch agencies—{[ ]}—as a failure to adequately "explain or rectify" the breaches identified by the Executive Branch agencies. The Executive Branch agencies assert, and we

[594] *Id*. (quoting ISPC Reclamation Letter at 1).

[595] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2108-09, April 4, 2019 Letter.

[596] *Id*., Business Confidential Exh. 103 at EB-2109, April 4, 2019 Letter.

[597] *Institution Order*, 35 FCC Rcd at 15039, para. 56 (quoting 2007 LOA at 2-3 (emphasis added) and citing Executive Branch Recommendation to Revoke and Terminate at 55).

[598] CTA Mar. 1, 2021 Reply at 31; *see also* CTA June 8, 2020 Response, Exh. 16 at 69-70. CTA argues that "[a]n interpretation of the LOA that requires prior notification to Team Telecom for trivial, ministerial filings with the FCC such as the ISPC assignment 'application' would be unreasonable and inconsistent with the intent of the agreement." CTA June 8, 2020 Response, Exh. 16 at 70. We disagree. As the Commission stated in the *Institution Order*, "[a] primary objective of the relevant 2007 LOA provision, and a material condition to the grant of the *pro forma* transfer of control in light of the Commission's reliance upon the views of the Executive Branch agencies, was to ensure that the Executive Branch agencies would be notified of [CTA's] dealings with the Commission, which did not happen here." *Institution Order*, 35 FCC Rcd at 15039, para. 56.

[599] 2007 LOA at 3.

[600] Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2108-09, April 4, 2019 Letter.

agree, that "[t]he evidence sufficiently demonstrates that [CTA] has not made good faith efforts to achieve compliance for more than a year."[601]

138. Finally, we continue to find unpersuasive CTA's argument that "even if the Commission did interpret the LOA to require such notification as the Recommendation urges, this 'breach' would be immaterial and insubstantial, and would not rise to the level of justifying revocation of section 214 authorizations or, for that matter, even a lesser sanction of some sort."[602] The action we take today relies on the entire record, which includes evidence showing that CTA failed to fulfill its various obligations under the 2007 LOA.

D. Further Mitigation Would Not Address National Security and Law Enforcement Concerns

139. Based on the record, we find that further 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 risks to national security and law enforcement interests.[603] The Executive Branch agencies, which have expertise in matters of national security and law enforcement and in monitoring carriers' compliance with risk mitigation agreements, state that "the underlying foundation of trust that is needed for a mitigation agreement to adequately address national security and law enforcement concerns is not present here."[604] We agree with the Executive Branch agencies that CTA "has proven to be an untrustworthy and unwilling partner in the Executive Branch's mitigation efforts under the existing LOA, a three-page document with only five key provisions . . . ."[605]

140. CTA 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 Executive Branch agencies' concerns. Instead, CTA merely restates its argument from its response to the *Order to Show Cause* that "'Team Telecom dictates mitigation measures to companies, essentially on a take-it-or-leave-it basis.'"[606] As discussed above, the evidence in the record shows that CTA had several opportunities to propose mitigation measures to the Executive Branch agencies.[607] CTA's arguments wholly ignore the

[601] Executive Branch Response at 7.

[602] CTA June 8, 2020, Response, Exh. 16 at 70; *see also Institution Order*, 35 FCC Rcd at 15040, para. 59 ("Particularly as applied to a company that is ultimately owned and controlled by the Chinese government, and in light of the national security and law enforcement concerns raised by the Executive Branch agencies concerning [CTA's] international section 214 authorizations, it is our view that serious concerns are raised by the breach of this provision of the 2007 LOA and by the record reflecting how [CTA] responded to the Executive Branch agencies' inquiries on this matter.").

[603] *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*, 35 FCC Rcd at 15017, para. 21.

[604] Executive Branch Recommendation to Revoke and Terminate at 53 (citing *China Mobile USA Order*, 34 FCC Rcd at 3380, para. 38).

[605] *Id*. The Executive Branch agencies have not indicated a change to their position concerning further mitigation in their subsequent filing. *See generally* Executive Branch Response.

[606] CTA Mar. 1, 2021 Reply at 29 (quoting CTA June 8, 2020 Response, Exh. 16 at 71).

[607] *See* Executive Branch Response at 7; *see, e.g.*, *supra* paras. 134, 137, note 539. As the Commission noted in the *Institution Order*, "[t]he record evidence shows that {[ ]} *Institution Order*, 35 FCC Rcd at 15041, para. 61 (quoting Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 102 at EB-2103 and citing *id.*, Business Confidential Exh. 119 at EB-2745-46); Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 102 at EB-2103, March 21, 2019 Letter ({[

(continued….)

specific national security and law enforcement risks identified by the Executive Branch agencies and do not address the concerns surrounding its ownership, access of its records by non-U.S. affiliates, and its vulnerability to exploitation, influence, and control by the Chinese government. Rather, CTA's arguments merely focus on the general difficulties of negotiating mitigation agreements with the Executive Branch agencies without a demonstration that they have attempted to do so.[608] Further, even if CTA had proposed additional mitigation terms or offered to renegotiate its LOA, the Executive Branch agencies have argued that such measures "would likely be insufficient to address newly discovered risks in today's rapidly evolving threat environment."[609]

141. We find that the record reflecting CTA's operation under the 2007 LOA and responses to the Executive Branch agencies' inquiries with respect thereto, combined with the national security and law enforcement risks that the Executive Branch agencies have now identified with regard to CTA's vulnerability to the exploitation, influence, and control of the Chinese government, raise serious concerns as to whether CTA can be trusted to cooperate with the Executive Branch agencies' mitigation monitoring in good faith and with transparency, and to comply with additional mitigation terms.[610] Based on the record, we agree with the Executive Branch agencies that CTA "should not be trusted to comply with more stringent mitigation measures."[611]

142. We also disagree with CTA's argument that "the [APA] seems to require that the Commission give CTA an opportunity to mitigate any risks that it might identify," and that the Commission has "to give CTA an 'opportunity to demonstrate or achieve compliance with all lawful requirements'" before revoking its authorizations.[612] *First*, as described above, this requirement is inapplicable in this case given the exception to this provision of the APA.[613] *Second*, the Executive Branch agencies have already given CTA several opportunities to negotiate further mitigation terms, and CTA has failed to do so, which demonstrates to the Commission that CTA acted willfully in breaching

(Continued from previous page)

]}); *id.*, Business Confidential Exh. 119 at EB-2745-46, May 29, 2019 Letter ({[

]}). In both March and May of 2019, the Executive Branch agencies afforded CTA opportunities to propose further mitigation measures, but CTA "failed to do so even though the [2007 LOA] came with fewer requirements than more recent Executive Branch mitigation agreements." Executive Branch Response at 7.

[608] *See, e.g.*, CTA Mar. 1, 2021 Reply at 29 ("As CTA previously explained, 'companies do not propose mitigation measure to Team Telecom. Team Telecom dictates mitigation measures to companies, essentially on a take-it-or-leave-it basis. Without being asked, CTA is unable to guess what potential new mitigation measures Team Telecom might consider adequate.'") (quoting CTA June 8, 2020 Response, Exh. 16 at 71)). However, CTA's own policies reflect {[

]} which calls into question CTA's statements concerning its interest in pursuing further mitigation terms or renegotiating the 2007 LOA. *See* Executive Branch Recommendation to Revoke and Terminate, Busines Confidential Exh. 37 at EB-655, January 24, 2019 Email.

[609] Executive Branch Recommendation to Revoke and Terminate at 55; *see also* CTA *Ex Parte* Letter at 2 (On October 8, 2021, CTA filed an *ex parte* letter stating that "it would be willing to consider accepting additional conditions, beyond those now contained in its letter of assurances, that would give the Executive Branch agencies greater visibility into its operations and greater safeguards against any 'perceived risks' they have identified, but the agencies have refused even to discuss the matter.").

[610] *Institution Order*, 35 FCC Rcd at 15041, para. 61.

[611] Executive Branch Recommendation to Revoke and Terminate at 55.

[612] CTA June 8, 2020 Response, Exh. 16 at 71; *see also* CTA *Ex Parte* Letter at 2 (stating, "even if the Executive Branch's opinions did constitute a potential ground for revocation, the Commission would still have to afford CTA and other respondents an opportunity to 'demonstrate or achieve compliance with all lawful requirements.'").

[613] *See supra* Section III.A.3.

the 2007 LOA and failing to engage the Executive Branch agencies to cure its breaches or ameliorate its compliance with the LOA.[614] Finally, CTA disagrees with our fundamental concerns in this proceeding—namely, concerns over CTA's ownership and control by the Chinese government raising substantial and unacceptable national security and law enforcement risks—and therefore no mitigation measures would be sufficient to address these concerns.[615]

E. Additional Evidence (Classified)

143. Although our decision to revoke the domestic authority and revoke and terminate the international authorizations issued to CTA, and the determination that further mitigation will not address the substantial national security and law enforcement risks, would be warranted based solely on the unclassified information in the record, a classified filing provided to the Commission by the Executive Branch agencies provides further support for our decision.

144. [616] [617] [618] [619] [620] [621] [622]

145. [623] [624] [625] [626] [627]

146. [628] [629]

147. [630] [631]

148. [632] [633]

[614] *See, e.g., supra* paras. 134, 137 & notes 539, 607-608.

[615] Based on our consideration of the totality of the evidence in the record and our findings herein with regard to CTA's section 214 authorizations, we reject CTA's claim that "the Executive Branch agencies seek indiscriminate revocation of the Section 214 authorizations held by all companies with controlling stock interests held by the People's Republic of China, regardless of any 'facts or conduct' relating directly to any given company, and based solely on their opinion as to the likely future actions of all such companies." CTA *Ex Parte* Letter at 2.

[616]

[617]

[618]

[619]

[620]

[621]

[622]

[623]

[624]

[625]

[626]

[627]

[628]

[629]

[630]

[631]

[632]

[633]

149. [634] [635]

150. [636] [637] [638]

151.

F. Transition Period

152. We direct CTA to discontinue all services relating to its section 214 authority no later than sixty (60) days from the release date of this Order. We require CTA 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. CTA may notify its MVNO customers in writing or by text message to their mobile number. In its letter or notification to its MVNO customers, CTA must certify its compliance with this requirement. We further require CTA 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 from this Order.[639]

153. We reject CTA's request to allow it at, a minimum, at least eighteen (18) months to allow for all customers to transition to other services should the Commission revoke and/or terminate its section 214 authority. In its reply, CTA argues that, in the event the Commission revokes or terminates its section 214 authority, the Commission must consider "the public interest in affording a reasonable transition period to users . . . in order to minimize disruption to business and other activities."[640] CTA claims that many of its MVNO customers have subscribed because of its Chinese-language customer service, that relatively few other carriers offer this type of customer service, and that finding a replacement service therefore will be more difficult for these customers than for the average MVNO customer.[641] CTA claims that in other cases the Commission has allowed for "even longer transition periods."[642]

154. Contrary to CTA's claims, the Commission's relevant discontinuance rules generally provide for much shorter transition periods than the requested minimum of eighteen (18) months. In 2007, the Commission amended its rules to require that a carrier with an international section 214 authorization shall notify customers at least thirty (30) days prior to a discontinuance of service.[643] The

---

[634]

[635]

[636]

[637]

[638]

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

[640] CTA Mar. 1, 2021 Reply at 59 (citing *Promoting Efficient Use of Spectrum Through Elimination of Barriers to the Development of Secondary Markets*, Report and Order and Further Notice of Proposed Rulemaking, 18 FCC Rcd 20604, 20679, para. 187 n.364 (2003), and "noting that revoking an authorization for a licensee that has leased its spectrum to another party 'will require the lessee to terminate its operations' and accounting for an appropriate transition period").

[641] *Id*. at 59.

[642] *Id*. at 60.

[643] Amendment of Parts 1 and 63 of the Commission's Rules, IB Docket No. 04-47, Report and Order, 22 FCC Rcd 11398, paras. 6-14 (2007).

Commission's previous rules, established in 1996, required a carrier to provide at least sixty (60) days of notice prior to discontinuance of a section 214 authorized international service.[644] The rules for discontinuance of a service by a carrier with domestic section 214 authority allow for discontinuance authority to be granted for non-dominant and dominant carriers, respectively, either thirty-one (31) or sixty (60) days after the application is accepted for filing.[645] In this instance, we find that a sixty (60) day transition period providing no less than thirty (30) days of written notice to customers[646] is most appropriate and should mitigate any difficulties CTA's customers may face in finding other providers that offer Chinese language customer support.[647] With regard to CTA's claim that the Commission has provided for longer transition periods in other cases, the examples cited reflect entirely different circumstances that are not relevant to the case at hand.[648] For example, in the case of the Commission's rules regarding unbundling and resale to which CTA cites, those rules while adopting longer transition periods involve the transition of competitive Local Exchange Carriers (CLECs) to other facilities or services or leasing the same facilities or services pursuant to new commercially-negotiated arrangements rather than regulated arrangements and are unrelated to discontinuance of service, much less discontinuance of service to achieve an important goal of the Commission to ensure the national security and law enforcement interests of the United States.[649]

155. 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. To assist CTA's MVNO customers with this transition, we will issue a consumer guide in English, Simplified Chinese, and Traditional Chinese on the Commission's website upon release of this Order and to any news outlets to advise consumers of our decision and to raise awareness of other options for mobile service.

---

[644] 40 CFR § 63.19. No comments were filed in opposition to this change from 60 to 30 days when the Commission considered the issue of notice for proposed discontinuances of international services in 2007.

[645] 47 CFR § 63.71(f)(1).

[646] *See id.*

[647] 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). CTA has not shown that its customers would be unable to obtain an adequate replacement service if the Commission revokes or terminates its section 214 authorizations.

[648] *See* CTA Mar. 1, 2021 Reply at 60 n.207.

[649] *Id*. at 60 (citing *Modernizing Unbundling and Resale Requirements in an Era of Next-Generation Networks and Services*, Report and Order, 35 FCC Rcd 12425, 12449, para. 46 (2020) (adopting a 42-month transition period for existing UNE DS1 Loops and a 36-month transition period for UNE DS3 Loops); *id.* at 12464-65, para. 75 (adopting a 48-month transition period for UNE DS0 Loops); *id*. at 12475-76, para. 95 (adopting a three-year transition period for UNE Narrowband Voice-Grade Loops); *Petition of USTelecom for Forbearance Pursuant to 47 U.S.C. § 160(c) to Accelerate Investment in Broadband and Next-Generation Networks*, Memorandum Opinion and Order, 34 FCC Rcd 6503, 6514-15, para. 23, 6526, paras. 45-46 (2019) (adopting a three-year transition period for UNE Analog Loops and Avoided-Cost Resale services to provide time for competitive LECs and their customers to transition to alternative service arrangements and avoid undue service disruptions); *Petition of USTelecom for Forbearance Pursuant to 47 U.S.C. § 160(c) to Accelerate Investment in Broadband and Next-Generation Networks*, Report and Order on Remand and Memorandum Opinion and Order, 34 FCC Rcd 5767, 5794-95, para. 60 (2019) (conditioning forbearance from UNE DS1/DS3 Transport obligations on a three-year transition period, taking into account "practical details of arranging for" alternative transport); *Revisions to Rules Authorizing the Operation of Low Power Auxiliary Stations in the 698-806 Mhz Band*, Report and Order and Further Notice of Proposed Rulemaking, 25 FCC Rcd 643, 652-53, para. 20 (2010) (providing a one-year transition period for low power auxiliary stations to cease operations in the 700 MHz Band)).

IV. ORDERING CLAUSES

156. 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 Telecom (Americas) Corporation's domestic section 214 authority is REVOKED and its international section 214 authorizations are REVOKED and TERMINATED.

157. IT IS FURTHER ORDERED that China Telecom (Americas) Corporation must discontinue all services relating to its section 214 authority no later than sixty (60) days from the release date of this Order.

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

China Telecom (Americas) Corporation
c/o Andrew D. Lipman
Catherine Wang
Russel M. Blau
Raechel Keay Kummer
Frank G. Lamancusa
Morgan, Lewis and Bockius LLP
1111 Pennsylvania Ave., NW
Washington, DC 20004

Luis Fiallo
Vice President
China Telecom (Americas) Corporation
607 Herndon Parkway, Suite 201
Herndon, VA 20170

Zhao-feng Ye
Director of Administration
China Telecom (Americas) Corporation
607 Herndon Parkway, Suite 201
Herndon, VA 20170

Jonathan Marashlian
DC Agent for Service of Process
The Commpliance Group, Inc.
1300 I Street, NW, Suite 400E
Washington, DC 20005

159. 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 Telecom (Americas) Corporation*, GN Docket No. 20-109; ITC-214-20010613-00346; ITC-214-20020716-00371; ITC-T/C-20070725-00285.

The Federal Communications Commission has a long history of working to open American markets to foreign telecommunications companies when doing so is in the public interest. These connections can make us stronger because they help share our democratic values with the rest of the world. But we also recognize not every connection is consistent with the national security interest of the United States. That's because some countries may seek to exploit our openness to advance their own national interests. When we recognize this is the case and cannot mitigate the risk, we need to take action to protect the communications infrastructure that is so critical to our national security and economic prosperity.

That is what we do here today. We take an important and necessary step to protect that infrastructure by revoking and terminating China Telecom Americas' authority to provide interstate and international telecommunications services in the United States.

This is not a decision we make lightly. It has support from each of my colleagues. It has support across the federal government. In fact, last year a broad group of Executive Branch agencies, including the Department of Justice, Department of Defense, Department of State, Department of Commerce, and the United States Trade Representative formally recommended that we terminate FCC authorization for China Telecom Americas to provide interstate and international telecommunications services in the United States. At about the same time, the Senate Permanent Subcommittee on Investigations issued a report on the threats that Chinese state-owned carriers pose to our telecommunications networks. In doing so, they highlighted a problem—that across the federal government there has not been enough oversight to safeguard our networks against evolving threats after issuance of a license.

That brings us to here and now. Since the Subcommittee on Investigations released its findings, the FCC has increased its oversight of telecommunications networks. That is why—following both regulatory and judicial review—we have reached the conclusion that it is necessary to terminate domestic and international Section 214 authority for China Telecom Americas. Our record makes clear that China Telecom Americas operates as a subsidiary of a Chinese state-owned enterprise and as such the Chinese government has the ability to influence and control its actions. That could lead to real problems with our telecommunications networks through surveilling information, misrouting traffic, or disrupting service. Moreover, the record reflects that China Telecom Americas has not been forthright in its representations to the FCC and other agencies. As a result, mitigation measures are not adequate to address our concerns and revocation of existing authorizations is justified.

This, however, is not the end of the story. Because our response to this provider, this one time, is not enough. As the Subcommittee on Investigations pointed out in its report, we need to work with our federal partners to ensure sufficient safeguards and oversight mechanisms are in place.

First, now that we have completed our review of China Telecom Americas, we are moving expeditiously to complete our security reviews for similarly situated carriers like China Unicom Americas, Pacific Networks, and ComNet.

Second, with this decision, we have established a clear precedent for revoking a foreign carrier's existing authorizations when there are national security concerns. Before today, that didn't exist. Now companies will understand the circumstances under which authorizations could be revoked and what due process is available to challenge potential revocations.

Third, consistent with the recommendations of the Subcommittee on Investigations, the FCC is coordinating with Executive Branch agencies on implementing periodic review of foreign carriers' authorizations to provide service in the United States. This will help ensure that we can stay on top of evolving national security, law enforcement, policy, and trade risks.

Fourth, the FCC is taking a closer look at applications for submarine cables to make sure they do not raise national security concerns. For too long, it was the practice of this agency to unilaterally grant applicants special temporary authority to start building submarine cables while their applications were pending, even if those applications reflected ownership by state-owned companies that could represent a national security risk. That's no longer the case. Requests for special temporary authority to start construction can raise national security concerns too, and the FCC now sends such requests to the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector for coordinated security review.

Thank you to the agency staff who worked on all of these efforts, but especially those who worked on this decision today, including Denise Coca, Kate Collins, Kim Cook, Francis Gutierrez, Jocelyn Jezierny, Gabrielle Kim, David Krech, Wayne Leighton, Adrienne McNeil, Tom Sullivan, and Troy Tanner from the International Bureau; Pamela Arluk, Michele Berlove, Melissa Droller Kirkel, Jodie May, Rodney McDonald, Kris Monteith, and Terri Natoli from the Wireline Competition Bureau; Jeffrey Gee, Rosemary Harold, Pamela Kane, and Christopher Killion from the Enforcement Bureau; Patrick Brogan, Robert Cannon, Matthew J. Collins, Cher Li, Kate Matraves, Giulia McHenry, Virginia Metallo, Donald Stockdale, and Emily Talaga from the Office of Economics and Analytics; Padma Krishnaswamy from the Office of Engineering and Technology; Kenneth Carlberg, Steven Carpenter, Lisa Fowlkes, Jeffery Goldthorp, Kurian Jacob, Debra Jordan, Lauren Kravetz, Nicole McGinnis, Saswat Misra, Zenji Nakazawa, Erika Olsen, and Austin Randazzo from the Public Safety and Homeland Security Bureau; Eduard Bartholme from the Consumer and Governmental Affairs Bureau; and, finally, Michele Ellison, Doug Klein, David Konczal, Jacob Lewis, Scott Noveck, Joel Rabinovitz, and Bill Richardson from the Office of General Counsel.

STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *China Telecom (Americas) Corporation*, GN Docket No. 20-109; ITC-214-20010613-00346; ITC-214-20020716-00371; ITC-T/C-20070725-00285.

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 security threats have evolved substantially in the intervening years. With that type of review in mind, the FCC opened investigations into several carriers, including China Telecom Americas, to assess any threats they pose to America's national security. While we continue our reviews of the other carriers, I am pleased that today we are bringing this one to a close. We are voting to revoke China Telecom America's domestic and international Section 214 authority.

Our decision today is informed by the views submitted by the Executive Branch agencies with responsibility for national security reviews. They advised that there are substantial and unacceptable national security and law enforcement risks associated with China Telecom Americas' continued access to U.S. telecommunications infrastructure. They also stated that China Telecom Americas' operations provide opportunities for Chinese state-sponsored actors to engage in espionage and to steal trade secrets and other confidential business information. Indeed, the FCC's own review found that China Telecom 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 that are contrary to the interests of the United States. Our review also found that China Telecom Americas' conduct towards the Commission and other agencies lacked candor and trustworthiness.

While today's vote is an important step forward, the FCC must remain vigilant to the threats posed by the Communist Party of China and those who would do its bidding. And on this score I have urged action on several fronts. First, we should quickly adopt final orders in our other section 214 investigations. Second, we should close the loophole in our equipment authorization process to ensure that equipment from Huawei and other entities that pose a national security risk will no longer be eligible for FCC approval. Just last week, the House passed legislation sponsored by Republican Whip Scalise and Congresswoman Eshoo that would require us to take this action. But there is no need for us to wait for that bill to become law. We can and should move quickly to close the Huawei loophole. Third, we need to ensure that we have a clear and efficient process in place for adding new entities to the FCC's Covered List.

Last week, I highlighted this issue as part of remarks where I called for the FCC to begin the process of adding DJI, a Shenzhen-based drone company, to the FCC's Covered List. As I laid out in a release, the evidence against DJI has been mounting for years, and various components of the U.S. government have taken a range of independent actions—including grounding fleets of DJI drones based on security concerns. Indeed, the Department of Defense affirmed just this past summer that DJI systems "pose potential threats to national security" and confirmed that they are still barred from general use by DoD. Yet a consistent and comprehensive approach to addressing DJI's potential threats is not in place. So the FCC should take the necessary steps to consider adding DJI to our Covered List. After all, we do not need a Huawei on wings.

Turning back to today's decision, this presents another opportunity to look at updating the agency's Covered List. The determinations reached by the Executive Branch agencies regarding China Telecom Americas appear sufficient to trigger the process of adding it to the FCC's Covered List under

our existing rules. So I would encourage the Commission to take that action, since it could impose additional restrictions on China Telecom Americas that go beyond the scope of our 214 authorizations.

Finally, I would like to thank staff from the International Bureau for their work on this item, as well as staff from across the various national security agencies who participated in this process. The item has my support.

STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *China Telecom (Americas) Corporation*, GN Docket No. 20-109; ITC-214-20010613-00346; ITC-214-20020716-00371; ITC-T/C-20070725-00285.

There are those out there who would attack our telecom networks. In just the last few months, we've learned about a hacker stealing the personal data of more than 50 million customers of a major American wireless carrier. We've read accounts of hackers penetrating the systems of a critical U.S. telecom backbone provider, gaining access to cellphone data for millions of users over a five-year period. And just last week, a cybersecurity research firm disclosed that hackers have been breaking into the computer networks of telecom companies across the world since 2016.

One of the reasons Congress created the FCC was to protect our networks from attacks like these. But even as hackers continue to attack our networks through the "back door," we face another threat from the "front door" – carriers that are owned or otherwise associated with adversary states. These companies seek or possess Commission authorizations to interconnect with U.S. networks and provide services within the U.S. to American citizens and foreign nationals. According to the Executive Branch agencies, with access to our networks and locations in our country, these companies can access, monitor, store, disrupt and misroute U.S. communications, misuse customer information, and facilitate espionage and other activities harmful to the United States.

Although we've acted against several such carriers, China Telecom Americas is a distinctly clear example of a company subject to the control of an adversary state. The company's parent is majority-owned and controlled by a Chinese government-owned enterprise. That parent company is directly accountable to the Chinese Communist Party and must consult with its representatives prior to making any decisions on material issues. And like other Chinese carriers, China Telecom Americas must disclose sensitive customer information whenever the Chinese government demands it.

Based on the information presented by the Executive Branch agencies, these risks are not theoretical. China Telecom Americas' U.S. records are already available to its non-U.S. affiliates abroad.[1] Moreover, according to public accounts, China Telecom Americas' network has misrouted large amounts of information and communications traffic outside of the United States over long periods, often for several months, and sometimes involving U.S. government traffic.[2] In addition, as detailed in this item, China Telecom Americas has a record of inaccurate representations to the FCC and other U.S. government agencies that demonstrates that it lacks the candor, trustworthiness, and reliability that we demand of our telecommunications carriers.[3] Based on the totality of these circumstances, our decision to revoke China Telecom Americas' section 214 authorizations is well-founded.

Thank you to the International Bureau and all the Commission staff that worked on this item for their hard work on this proceeding.

[1] *See* Order on Revocation and Termination at para. 69.

[2] *See id.* at para. 88.

[3] *See id.* at para. 2.