

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 INSTITUTING PROCEEDINGS ON REVOCATION AND TERMINATION AND
MEMORANDUM OPINION AND ORDER

Adopted: December 10, 2020

Released: December 14, 2020

By the Commission: Chairman Pai, Commissioners Carr and Starks issuing separate statements.

TABLE OF CONTENTS

Heading Paragraph #
I. INTRODUCTION..... 1
II. BACKGROUND..... 2
III. ORDER INSTITUTING PROCEEDINGS..... 15
A. Revocation of Section 214 Authority..... 20
1. National Security and Law Enforcement Concerns Related to China Telecom
Americas..... 22
2. National Security and Law Enforcement Risks Associated with China Telecom
Americas’ Retention of Section 214 Authorities..... 29
3. China Telecom Americas’ Past Conduct and Representations to the Executive Branch
Agencies..... 37
4. The Executive Branch Agencies Do Not Recommend Further Mitigation..... 44
B. Termination of International Section 214 Authorizations 47
IV. MEMORANDUM OPINION AND ORDER 62
V. PROCEDURAL MATTERS..... 71
VI. ORDERING CLAUSES..... 76

I. INTRODUCTION

1. In this Order, we institute proceedings to revoke the domestic authority and revoke and/or terminate the international authorizations issued to China Telecom (Americas) Corporation (China Telecom Americas) pursuant to section 214 of the Communications Act of 1934, as amended (Act).¹ We find that China Telecom Americas has failed to rebut the serious concerns of the Executive Branch about its continued presence in the United States and thus adopt procedures that will allow for China Telecom

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, EB 2020) (Order to Show Cause); China Telecom (Americas) Corporation, Response 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) (China Telecom Americas Response) (filing with the Commission a public filing and a non-public business confidential filing).

Americas, Executive Branch agencies, and the public to present any remaining arguments or evidence in this matter. Specifically, we deny an Application for Review filed by China Telecom Americas and direct the International Bureau to provide to the Department of Justice, in its capacity as chair of the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Committee), information submitted in confidence by China Telecom Americas, so that it may fully participate in this proceeding.² We then provide the public and the Committee with forty (40) days to respond to China Telecom Americas' June 8, 2020, filing. China Telecom Americas will then have forty (40) days thereafter to present arguments and evidence in reply—at which point the record in this proceeding will be complete and ready for final adjudication by the Commission.

II. BACKGROUND

2. Congress created the Commission, among other reasons, “for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communications”³ Promotion of national security is an integral part of the Commission’s public interest responsibility, including in connection with its administration of section 214 of the Act,⁴ and indeed one of the core purposes for which Congress created the Commission.⁵ The Commission has taken a number of targeted steps to protect the nation’s communications infrastructure from potential security threats recently,⁶ and we continue to do so here.

3. *Revocation of Domestic and International Section 214 Authority.* Section 214(a) of the Act prohibits any carrier from constructing, extending, acquiring, or operating any line, and from engaging in transmission through any such line, without first obtaining a certificate from the Commission “that the present or future public convenience and necessity require or will require the construction, or operation, or construction and operation, of such additional or extended line”⁷ In granting domestic

² China Telecom (Americas) Corporation, Application for Review of China Telecom (Americas) Corporation, GN Docket No. 20-109, ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (filed Aug. 31, 2020) (Application for Review).

³ 47 U.S.C. § 151.

⁴ 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*).

⁵ See *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs et al.*, WC Docket No. 18-89 et al., Report and Order, Further Notice of Proposed Rulemaking, and Order, 34 FCC Rcd 11423, 11436, para. 34 (2019) (*Protecting Against National Security Threats Order*), *appeal pending in Huawei Technologies USA v. FCC*, No. 19-60896 (5th Cir.); *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, 35 FCC Rcd 7821, 7822, para. 5 (2020) (*Protecting Against National Security Threats Declaratory Ruling and Second Further Notice*).

⁶ 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, para. 27; see generally *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, FCC 20-176 (Dec. 11, 2020).

⁷ 47 U.S.C. § 214(a). The Supreme Court has determined that the Commission has considerable discretion in deciding how to make its section 214 public interest finding. *FCC v. RCA Communications, Inc.*, 346 U.S. 86, 90 (1953); see also *Policy and Rules Concerning Rates for Competitive Common Carrier Services and Facilities*

(continued....)

section 214 authority by rule,⁸ 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.⁹ 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.¹⁰ The Commission has initiated revocation proceedings concerning section 214 authorizations in different contexts.¹¹

4. As part of the Commission’s public interest analysis, the Commission considers a number of factors and examines the totality of the circumstances in each particular situation. One of the factors is whether the application for or retention of the authorization raises any national security, law enforcement,

(Continued from previous page) _____

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).

⁸ In 1999, the Commission granted all telecommunications carriers blanket authority under section 214 of the Act to provide domestic interstate services and to construct or operate any domestic transmission line. *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.

⁹ *Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11374, para. 16.

¹⁰ See, e.g., *Foreign Participation Order*, 12 FCC Rcd at 24023, para. 295 (where the Commission finds that a U.S. carrier has engaged in anticompetitive conduct); *Reconsideration Order*, 15 FCC Rcd at 18173, para. 28 (where the Commission finds that a U.S. carrier has acquired an affiliation with a foreign WTO carrier and such affiliation poses a very high risk to competition that cannot be remedied by safeguards); *id.* at 18175-76, para. 35 (where the Commission finds that a U.S. carrier has proposed to acquire a controlling interest in a foreign non-WTO carrier that does not satisfy the effective competitive opportunities (ECO) test or the affiliation may otherwise harm the public interest pursuant to the Commission’s policies and rules); see also 47 CFR § 63.11(g)(2); *Reform of Rules and Policies on Foreign Carrier Entry Into the U.S. Telecommunications Market*, IB Docket No. 12-299, Report and Order, 29 FCC Rcd 4256, 4259, 4266, paras. 6, 22 (2014) (eliminating the ECO test which, among other things, had applied to international section 214 applications filed by foreign carriers or their affiliates that have market power in non-WTO Member countries they seek to serve and to notifications filed by authorized U.S. carriers affiliated with or seeking to become affiliated with a foreign carrier that has market power in a non-WTO Member country that the U.S. carrier is authorized to serve, while continuing to reserve the right to proceed to an authorization revocation hearing if the Commission finds that the affiliation may harm the public interest).

¹¹ See, e.g., *CCN, Inc. et al.*, Order to Show Cause and Notice of Opportunity for Hearing, 12 FCC Rcd 8547 (1997); *CCN, Inc. et al.*, Order, 13 FCC Rcd 13599 (1998) (revoking a company’s operating authority under section 214 for repeatedly slamming consumers); *Rates for Interstate Inmate Calling Services*, Report and Order and Further Notice of Proposed Rulemaking, 28 FCC Rcd 14107, 14170, para. 118 (2013); *Lifeline and Link Up Reform and Modernization et al.*, Report and Order and Further Notice of Proposed Rulemaking, 27 FCC Rcd 6656, 6785, para. 299 (2012); *Kurtis J. Kintzel et al.; Resellers of Telecommunications Services*, Order to Show Cause and Notice of Opportunity for Hearing, 22 FCC Rcd 17197, 17197, 17204-05, 17205-07, paras. 1, 22, 24 (2007); *Compass, Inc.; Apparent Liability for Forfeiture*, Notice of Apparent Liability for Forfeiture and Order, 21 FCC Rcd 15132, 15141-42, para. 29 (2006).

foreign policy, or trade policy concerns related to the applicant's or authorization holder's reportable foreign ownership.¹²

5. With regard to national security, law enforcement, foreign policy, or trade policy concerns related to certain applications that have reportable foreign ownership, 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.¹³ We recently formalized the review process for the Executive Branch agencies to complete their review consistent with the President's April 4, 2020 Executive Order No. 13913 that established the Committee.¹⁴ The Commission ultimately makes an independent decision in light of the information in the record, including any information provided by the applicant, authorization holder, or licensee in response to any filings by the Executive Branch agencies.¹⁵

6. China Telecom Americas is a Delaware corporation that is indirectly and ultimately owned and controlled by the government of the People's Republic of China.¹⁶ China Telecom Americas is a direct, wholly owned subsidiary of China Telecom Corporation Limited, an entity that is listed on the Hong Kong Stock Exchange and New York Stock Exchange.¹⁷ China Telecom Corporation Limited is incorporated in the People's Republic of China.¹⁸ China Telecommunications Corporation (China Telecom), a corporation organized under Chinese law, holds, as of April 30, 2020, approximately 70.89%

¹² See *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66; see also *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*).

¹³ *Foreign Participation Order*, 12 FCC Rcd at 23918-21, paras. 59-66. In the 1997 *Foreign Participation Order*, the Commission affirmed its previously *ad hoc* policy of seeking Executive Branch input on any national security, law enforcement, foreign policy, or trade policy concerns related to the reportable foreign ownership as part of its overall public interest review of an application. The policy also applies to other types of applications with reportable foreign ownership, including applications related to submarine cable landing licenses, assignments or transfers of control of domestic or international section 214 authority, and petitions for declaratory rulings to exceed the foreign ownership benchmarks of section 310(b) of the Act. *Id.*; *Amendment of the Commission's Regulatory Policies to Allow Non-U.S. Licensed Space Stations to Provide Domestic and International Satellite Service in the United States et al.*, IB Docket No. 96-111 et al., Report and Order, 12 FCC Rcd 24094, 24171, paras. 179-80 (1997); see also *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10928-30, paras. 3-7.

¹⁴ See generally *Executive Branch Process Reform Report and Order*; Executive Order No. 13913 of April 4, 2020, Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, 85 Fed. Reg. 19643 (Apr. 8, 2020) (Executive Order 13913) (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).

¹⁵ *Foreign Participation Order*, 12 FCC Rcd at 23921, para. 66 ("We emphasize that the Commission will make an independent decision on applications to be considered and will evaluate concerns raised by the Executive Branch agencies in light of all the issues raised (and comments in response) in the context of a particular application.").

¹⁶ China Telecom Americas Response, Exh. 1 at 1; *Order to Show Cause*, 35 FCC Rcd at 3715, para. 6. China Telecom Americas 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).

¹⁷ China Telecom Americas Response, Exh. 1 at 1; *Order to Show Cause*, 35 FCC Rcd at 3716, para. 6.

¹⁸ China Telecom Americas Response, Exh. 1 at 1; *Order to Show Cause*, 35 FCC Rcd at 3716, para. 6.

of the outstanding shares of China Telecom Corporation Limited.¹⁹ The remaining outstanding shares are held by: (1) entities registered or organized under the laws of the People's Republic of China (11.96%)²⁰ and (2) shareholders trading on the public exchange (17.15%).²¹ China Telecom is 100% directly owned by the State-owned Assets Supervision and Administration Commission of the State Council, a Chinese government organization.²²

7. According to China Telecom Americas, 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.”²³ China Telecom Americas 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.”²⁴

8. China Telecom Americas holds two international section 214 authorizations, ITC-214-20010613-00346 and ITC-214-20020716-00371, which are conditioned on China Telecom Americas abiding by the commitments and undertakings contained in its July 17, 2007 letter of assurances (LOA) to the Department of Justice (DOJ), including the Federal Bureau of Investigation (FBI), and Department of Homeland Security (DHS)²⁵ (2007 LOA).²⁶ Additionally, it provides domestic interstate

¹⁹ China Telecom Americas Response, Exh. 1 at 1; *Order to Show Cause*, 35 FCC Rcd at 3716, para. 6.

²⁰ 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%). China Telecom Americas Response, Exh. 1 at 1.

²¹ The shareholders trading on the public exchange include Citigroup, Inc.; BlackRock, Inc.; GIC Private Limited; the Bank of New York Mellon Corporation; JPMorgan Chase & Co.; and Franklin Resources, Inc. China Telecom Americas Response, Exh. 1 at 1.

²² *Id.*, Exh. 1-1; *id.*, Exh. 1 at 1 (“[China Telecom] 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.

²³ China Telecom Americas Response, Exh. 6 at 1. A complete procedural history of China Telecom Americas' authorizations can be found in the *Order to Show Cause*. *Order to Show Cause*, 35 FCC Rcd at 3714-15, paras. 2-4.

²⁴ China Telecom Americas Response, Exh. 6 at 1. China Telecom Americas states that it provides international private leased circuits; International Ethernet Private Line service; Global Wavelength service; Ethernet over MPLS (EoMPLS); Multiple Protocol Label Switching/Virtual Private Network (MPLS-VPN) service; Internet Protocol Security VPN service; Global Internet Service using both ChinaNet and CN2; mobile virtual network operator (MVNO) services; and SIP trunking service. *Id.* at 2-6. China Telecom Americas also states that it provides the following other services, which it argues are not telecommunications services: Internet Data Center Services; Cloud Service; Virtual Private Cloud; Cloud Exchange; SD-WAN; customer premises equipment; equipment leasing; Project Item service; connectivity monitoring and network troubleshooting; Maintenance Service; Anti-DDOS service; Global Media Distribution and Exchange; and professional Information and Communications Technologies services. *Id.* at 6-9.

²⁵ 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 at 1 (July 17, 2007) (on file in ITC-T/C-20070725-00285).

²⁶ The 2007 LOA requires China Telecom Americas 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 (continued....)

telecommunications service²⁷ pursuant to blanket section 214 authority that the Commission has issued by rule.²⁸

9. 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 China Telecom Americas' international section 214 authorizations.²⁹ The Executive Branch agencies that jointly made this recommendation are DOJ, DHS, the Departments of Defense, State, and Commerce, and the United States Trade Representative.³⁰ 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 [China Telecom Americas’] continued access to U.S. telecommunications infrastructure pursuant to its international Section 214 authorizations.”³¹ The Executive Branch Recommendation to Revoke and Terminate is based on changed circumstances in the national security environment, including the U.S. government’s increased concern in recent years about the Chinese government’s malicious cyber activities; China Telecom Americas’ status as a subsidiary of a Chinese state-owned enterprise under the ultimate ownership and control of the Chinese government; China Telecom Americas’ representations to U.S. government authorities and U.S. customers regarding its cybersecurity practices, and its apparent failure to comply with U.S. federal and state cybersecurity and privacy laws; China Telecom Americas’

(Continued from previous page) _____
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 [China Telecom Americas] 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.

²⁷ China Telecom Americas 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.

²⁸ 47 CFR § 63.01. The Commission explained that it grants blanket section 214 authority, rather than forbearing from application or enforcement of section 214 entirely, in order to retain its ability to withdraw such grants on an individual basis for enforcement purposes. *Domestic 214 Blanket Authority Order*, 14 FCC Red at 11372-73, 11374, paras. 12-14, 16.

²⁹ Executive Branch Recommendation to the Federal Communications Commission to Revoke and Terminate [China Telecom Americas’] International Section 214 Common Carrier Authorizations, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (filed Apr. 9, 2020) (Executive Branch Recommendation to Revoke and Terminate) (filing with the Commission a public filing, a non-public business confidential filing, and a classified appendix).

³⁰ *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 recently 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.”

³¹ Executive Branch Recommendation to Revoke and Terminate at 1.

alleged noncompliance with the terms of the 2007 LOA issued as a condition of the International Bureau's grant of the *pro forma* transfer of control of its international section 214 authorizations; and China Telecom Americas' U.S. operations, which provide opportunities for increased Chinese state-sponsored cyber activities, including economic espionage and the disruption and misrouting of U.S. communications traffic.³² The Executive Branch agencies add that “[i]n the current environment, the national security and law enforcement risks associated with [China Telecom Americas’] international Section 214 authorizations cannot be mitigated.”³³ 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.”³⁴

10. On April 9, 2020, DOJ filed notice of its intent to use Foreign Intelligence Surveillance Act (FISA) information pursuant to 50 U.S.C. § 1806(c) “in any proceedings” regarding the Executive Branch Recommendation to Revoke and Terminate.³⁵ On May 1, 2020, China Telecom Americas, by its counsel, filed a letter requesting that the Commission “disclose to [China Telecom Americas] any and all FISA-related, obtained, or derived information related to [China Telecom Americas] in the Commission’s possession.”³⁶

11. On April 24, 2020, the International Bureau, Wireline Competition Bureau, and Enforcement Bureau (the Bureaus) issued the *Order to Show Cause* directing China Telecom Americas to file a response within thirty (30) calendar days demonstrating why the Commission should not initiate a proceeding to revoke and terminate China Telecom Americas’ domestic and international section 214 authorizations.³⁷ Among other things, the Bureaus noted the views of the Executive Branch agencies that

³² *Id.*

³³ *Id.* at 2.

³⁴ *Id.*

³⁵ Notice by the U.S. Department of Justice of Intent to Use Foreign Intelligence Surveillance Act Information, China Telecom (Americas) Corporation f/k/a China Telecom (USA) Corporation, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, at 1 (Apr. 9, 2020).

³⁶ Letter from Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP, to Ajit Pai, Chairman, FCC at 2 (May 1, 2020) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285). China Telecom Americas also requested that the Commission disclose, “to the extent known by the Commission, (a) the length of time that the government has engaged in surveillance of [China Telecom Americas], and/or its agents, (b) the identity of any individual who has been surveilled, and (c) the methods of surveillance.” *Id.* China Telecom Americas requested “access to the above mentioned FISA-related, obtained or derived information and classified appendix in the Commission’s possession so that [China Telecom Americas] may promptly respond to the Order to Show Cause.” *Id.* On December 8, 2020, the Department of Justice filed in this docket a notice “that the United States has recently initiated a proceeding against [China Telecom Americas] 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 (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); see *United States v. China Telecom (Americas) Corp.*, Case No. 20-mc-116, ECF No. 1 (D.D.C. filed Nov. 24, 2020).

³⁷ See generally *Order to Show Cause*; see also *id.*, 35 FCC Rcd at 3718, 3720, paras. 12, 14. In the *Order to Show Cause*, the Bureaus also asked China Telecom Americas to explain why the Commission should not reclaim China Telecom Americas’ three International Signaling Point Codes (ISPCs). *Id.* On November 18, 2020, based on the information China Telecom Americas filed in response to the *Order to Show Cause*, the International Bureau found that China Telecom Americas was not in compliance with the conditions of its provisional ISPC assignments, and reclaimed the three ISPCs. Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC

(continued....)

there are “substantial and unacceptable national security and law enforcement risks associated with [China Telecom Americas’] continued access to U.S. telecommunications infrastructure pursuant to its international Section 214 authorizations.”³⁸ The *Order to Show Cause* also directed China Telecom Americas to respond to certain questions concerning its ownership, operations, and other related matters, to provide “a description of the extent to which China Telecom Americas 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].”³⁹ On June 8, 2020, China Telecom Americas filed its response to the *Order to Show Cause*, including a public filing and a non-public business confidential filing.⁴⁰

12. *Request for Disclosure of China Telecom Americas’ Confidential Business Information.* 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 China Telecom Americas had requested confidential treatment.⁴¹ DOJ stated that it intends on sharing the information with the Members of and Advisors to the Committee.⁴² China Telecom Americas objected to the disclosure, contending, among other things, that DOJ and the Committee have not established a legitimate need for the requested information.⁴³ According to China Telecom Americas, the *Order to Show Cause* “makes no

(Continued from previous page)

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). China Telecom Americas admitted that ISPC {[]} has not been in use since {[]} was “not ultimately configured for use.” *Id.* at 1; China Telecom Americas Response, Exh. 9 at 1-2; *see also* 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). China Telecom Americas 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.

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

³⁸ *Order to Show Cause*, 35 FCC Rcd at 3713, para. 1.

³⁹ *Id.* at 3718-19, para. 12.

⁴⁰ China Telecom Americas Response. On April 27, 2020, China Telecom Americas filed a motion for an extension of the time for its response to the *Order to Show Cause*, seeking an additional 30 days, to June 23, 2020, or, if this is not possible, then to June 8, 2020. China Telecom (Americas) Corporation, Motion for Extension of Time, GN Docket No. 20-109 et al., at 1, 3 (filed Apr. 27, 2020) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285). On May 14, 2020, the International Bureau’s Telecommunications and Analysis Division granted China Telecom Americas an extension of time to respond to June 8, 2020. Letter from Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau, to Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP, 35 FCC Rcd 4881 (May 14, 2020) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285).

⁴¹ Letter from Sanchitha Jayaram, Chief, Foreign Investment Review Section, National Security Division, U.S. Department of Justice, to Denise Coca, Chief, Telecommunications and Analysis Division, FCC International Bureau (July 8, 2020) (Department of Justice July 8, 2020 Letter) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285).

⁴² *Id.* at 2.

⁴³ Letter from Andrew D. Lipman, Counsel to China Telecom (Americas) Corporation, Morgan, Lewis & Bockius LLP, to Marlene Dortch, Secretary, FCC at 2-3 (July 27, 2020) (on file in GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285).

provision for the Committee to ‘respond fully’ or at all to [China Telecom Americas’] response to the Executive Branch’s recommendation,” and therefore DOJ and the Committee do not need access to the confidential information.⁴⁴

13. On August 17, 2020, the International Bureau informed China Telecom Americas that pursuant to section 0.442 of the Commission’s regulations,⁴⁵ 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 China Telecom Americas, subject to the provisions of 44 U.S.C. § 3510(b).⁴⁶

14. On August 31, 2020, China Telecom Americas filed an Application for Review contending, among other things, that (1) “[t]he International Bureau lacks the authority to grant DOJ’s request for the disclosure of certain confidential information submitted by [China Telecom Americas] to the Commission” and (2) “[t]he International Bureau decision that DOJ established a legitimate need for the confidential material was erroneous.”⁴⁷ Because we have not yet addressed this Application for Review, the information for which China Telecom Americas sought confidential treatment has not been disclosed to DOJ or to the Committee.

III. ORDER INSTITUTING PROCEEDINGS

15. Based on our public interest analysis under section 214 of the Act and the totality of the record evidence,⁴⁸ we find that more than sufficient cause exists to initiate a proceeding on whether to revoke and terminate China Telecom Americas’ domestic and international section 214 authority, and we do so herein. To allow China Telecom Americas to respond to the serious concerns raised by the Executive Branch agencies, which seem to justify revocation of China Telecom Americas’ section 214 authority, we afford China Telecom Americas a further opportunity to show cause why the public interest, convenience, and necessity do not warrant revocation of its domestic section 214 authority and international section 214 authorizations, and/or termination of its international section 214 authorizations due to its failure to comply with terms of its mitigation agreement. We therefore adopt procedures to finalize the Commission’s adjudication of the issues presented in this matter. Following its review of the record, the Commission will determine whether the record as a whole supports revocation and/or termination of China Telecom Americas’ section 214 authority.⁴⁹ We also deny China Telecom

⁴⁴ *Id.* at 2.

⁴⁵ 47 CFR § 0.442.

⁴⁶ *China Telecom (Americas) Corporation*, GN Docket No. 20-109, File Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285, Letter Order, 35 FCC Rcd 8775 (IB 2020) (Disclosure Ruling).

⁴⁷ Application for Review at 2, 4.

⁴⁸ The Commission takes official notice of the Recommendation and the classified information submitted by the Executive Branch agencies with its Recommendation. *See* 47 U.S.C. § 154(j); *Use of Classified Information; Policy to be Followed in Future Licensing of Facilities for Overseas Communications*, Order, FCC 78-755, 44 Rad. Reg. 2d 607, 611, para. 10 (1978).

⁴⁹ We note that, contrary to the assertion of China Telecom Americas, it is now well established 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. *See* 5 U.S.C. § 556(d) (“[A] sanction may not be imposed . . . except on consideration of the whole record or those parts thereof cited by a party and supported by and in accordance with the reliable, probative, and substantial evidence.”); *Steadman v. SEC*, 450 U.S. 91, 101 & n. 21 (1981) (citing *Sea Island Broadcasting v. FCC*, 627 F.2d 240 (D.C. Cir. 1980)); *In re Kay*, 17 FCC Rcd 1834, 1837, para. 11 (2002) (subsequent history omitted). We invite the parties to address this question further in their subsequent filings.

Americas' pending Application for Review and direct the International Bureau to promptly produce to DOJ and the Committee the information submitted in confidence by China Telecom Americas so that these entities may fully participate in this process.

16. We initiate these further proceedings to determine whether to revoke the domestic section 214 authority and whether to revoke and/or terminate the international section 214 authorizations held by China Telecom Americas.⁵⁰ This proceeding affords China Telecom Americas 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. In accordance with the Commission's well-established authority to "conduct its proceedings in such manner as will best conduce to the proper dispatch of business and to the ends of justice,"⁵¹ the Commission establishes procedures for the submission of additional filings, described below, which we judge sufficient to ascertain whether revocation and/or termination would be consistent with the public interest, convenience, and necessity.

17. We find that these additional procedures are consistent with both principles of due process and applicable law. China Telecom Americas has suggested that, if the Commission initiates a proceeding to revoke its authorizations, "such proceeding must be an adjudicatory hearing before an Administrative Law Judge."⁵² We disagree. In our judgment, there are no substantial and material questions of fact in this case warranting an adjudicatory hearing before an Administrative Law Judge or other presiding officer. The written record is already extensive, and China Telecom Americas will have a further opportunity to respond to this Order and to any additional evidence or arguments that may be submitted. The record includes information submitted by the Executive Branch agencies that has been classified for national-security reasons and will not be made available to China Telecom Americas,⁵³ and we note that it is well established that neither the Administrative Procedure Act (APA)⁵⁴ nor due process requires disclosure of such material.⁵⁵

18. The Bureaus' *Order to Show Cause* provided China Telecom Americas with any notice and opportunity that may be required by 5 U.S.C. § 558 before the institution of a proceeding to revoke its authority, though it appears from the record that "the public . . . interest, or safety" may require revocation in any event.⁵⁶ Nothing in the APA requires the application of trial-type procedures to the ensuing proceeding even when section 558 applies.⁵⁷

⁵⁰ See 47 U.S.C. §§ 154(j), 403; 47 CFR § 1.1.

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

⁵² China Telecom Americas Response at 6.

⁵³ See 47 U.S.C. § 154(j) (authorizing the Commission to protect classified information).

⁵⁴ 5 U.S.C. §§ 551-559.

⁵⁵ See, e.g., *Jifry v. FAA*, 370 F.3d 1174, 1184 (D.C. Cir. 2004). To the extent the Commission ultimately determines to rely on any classified information as necessary to support that determination, such classified information may be reviewed by a reviewing court *in camera*. See *id.* at 1183.

⁵⁶ 5 U.S.C. § 558(c). In addition, the requirements of section 558(c) do not apply "in cases of willfulness." Here, China Telecom Americas has acted willfully in taking the actions identified in the Executive Branch

(continued....)

19. Finally, China Telecom Americas is not correct in its argument that revocation requires a finding of an egregious violation of a specific requirement.⁵⁸ Whereas a revocation or license cancellation that is based solely on a violation of a specific requirement may indeed require that the agency find such a violation, in this case, revocation would be based upon an assessment of the public interest, convenience, and necessity under section 214 of the Act, which may be affected by other considerations, including but not limited to considerations outside the authorization holder's control. Even a Title III (wireless) license may be revoked because of conditions coming to the attention of the Commission that would have warranted a refusal to grant a license on an original application.⁵⁹ The 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"⁶⁰ and explained that it grants "blanket" and "global" authorizations with the understanding that they may be revoked.⁶¹ China Telecom Americas argues that the 1997 *Foreign Participation Order* stated that a section 214 authorization could be revoked only in cases of adjudicated misconduct.⁶² It would be unreasonable, however, to conclude that adjudicated misconduct could be the only justification for revocation, either where necessary "to prevent competitive harm in the U.S. market"⁶³ or for "[n]ational security and law enforcement concerns . . . independent of our competition analysis"⁶⁴ that also form an integral part of the Commission's public interest analysis and are specifically reserved under the WTO Basic Telecom Agreement.⁶⁵

A. Revocation of Section 214 Authority

20. With regard to the revocation of China Telecom Americas' domestic and international section 214 authority, we consider whether the domestic section 214 authority and international section 214 authorizations continue to serve the public interest, convenience, and necessity, as the Commission found to be the case when it granted blanket domestic section 214 authority to carriers entering the domestic U.S. market and consistent with the inquiry conducted at the time the International Bureau first granted China Telecom Americas the international section 214 authorizations.⁶⁶ We institute this further

(Continued from previous page) _____
Recommendation to Revoke and Terminate. *See Coosemans Specialties, Inc. v. Dep't of Agriculture*, 482 F.3d 560, 567-68 (D.C. Cir. 2007) (holding that an act is "willful" for purposes of section 558 if done "intentionally, irrespective of evil intent, or done with careless disregard of statutory requirements").

⁵⁷ *Empresa Cubana Exportadora de Alimentos Y Productos Varios v. U.S. Dep't of the Treasury*, 638 F.3d 794, 802 (D.C. Cir. 2011) (Kavanaugh, J.) (citing *Gallagher & Ascher Co. v. Simon*, 687 F.2d 1067, 1073-75 (7th Cir. 1982)).

⁵⁸ China Telecom Americas Response, Exh. 16 at 8-11.

⁵⁹ 47 U.S.C. § 312(a)(2).

⁶⁰ *Foreign Participation Order*, 12 FCC Rcd at 23900, para. 19.

⁶¹ *See Domestic 214 Blanket Authority Order*, 14 FCC Rcd at 11372-73, 11374, paras. 12-14, 16; *see also 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.").

⁶² China Telecom Americas Response, Exh. 16 at 8-9 (citing *Foreign Participation Order*, 12 FCC Rcd 23891, 24023, para. 295, and *Marpin Telecoms and Broadcasting Company Limited v. Cable & Wireless, Inc.*, 18 FCC Rcd 508, 515 (2003)).

⁶³ *Foreign Participation Order*, 12 FCC Rcd at 24022-23, paras. 293-296.

⁶⁴ *Id.* at 23919, 23921, paras. 63, 65.

⁶⁵ *Id.* at 24039, para. 341 & n.696; *id.* at 24043, para. 351; *id.* at 24048-49, para. 364.

⁶⁶ *See* 47 U.S.C. §§ 154(i), 214.

proceeding because of concerns that China Telecom Americas' ownership and control by the Chinese government raise substantial and unacceptable national security and law enforcement risks regarding its domestic section 214 authority and international section 214 authorizations that cannot be addressed through further mitigation with the Executive Branch agencies. In particular, we seek to address concerns that China Telecom Americas' ties to the Chinese government—together with Chinese laws obligating China Telecom Americas and its direct and indirect parent entities and affiliates to cooperate with any request by the Chinese government to use or access their systems—pose a clear and imminent threat to the security of the United States due to their access to U.S. telecommunications infrastructure.⁶⁷

21. The Executive Branch agencies advise that there are now substantial and unacceptable national security and law enforcement risks associated with China Telecom Americas' continued access to U.S. telecommunications infrastructure.⁶⁸ We find that China Telecom Americas has not adequately demonstrated to the contrary. Based on the record, China Telecom Americas is ultimately owned and controlled by the Chinese government, and due to this relationship, China Telecom Americas may be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight.⁶⁹ Further, it appears that China Telecom Americas' U.S. operations provide opportunities for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic.⁷⁰ China Telecom Americas has not adequately responded to the Executive Branch agencies' concerns that China Telecom Americas' lack of trustworthiness limits the Executive Branch agencies' ability to conduct statutorily authorized law enforcement and national security missions.⁷¹ The Executive Branch agencies, which have expertise in matters of national security and law enforcement and in monitoring carriers' compliance with risk mitigation agreements, advise that further mitigation would be insufficient to overcome their concerns.⁷² We have a longstanding policy of according deference to their expertise in mitigating risks to national security and law enforcement interests. Based on the substantial national security and law enforcement concerns raised by the Executive Branch agencies and the evidence in the record, it appears that the public interest requires revocation of China Telecom Americas' section 214 authority.

1. National Security and Law Enforcement Concerns Related to China Telecom Americas

22. The Executive Branch agencies state that “[l]ike the applicant in [the] *China Mobile [USA Order]*, [China Telecom Americas] is indirectly majority-owned and controlled by the Chinese government and is vulnerable to exploitation, influence and control by the Chinese government.”⁷³ They further state that China Telecom Americas is “wholly owned and controlled by a single Chinese entity,” China Telecom Corporation Limited, which is “majority-owned and controlled by a state-owned enterprise under Chinese government supervision.”⁷⁴ Significantly, in January 2018, China Telecom Corporation Limited revised its Articles of Association to give the Chinese Communist Party greater

⁶⁷ See *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11433, 11442, paras. 27, 49.

⁶⁸ Executive Branch Recommendation to Revoke and Terminate at 1.

⁶⁹ *Id.* at 32, 37; see also *China Mobile USA Order*, 34 FCC Rcd at 3368-69, 3371, paras. 14, 16, 19.

⁷⁰ Executive Branch Recommendation to Revoke and Terminate at 41.

⁷¹ *Id.* at 51.

⁷² *Id.* at 53.

⁷³ *Id.* at 34.

⁷⁴ *Id.*

control over the management and operations of China Telecom Corporation Limited’s business.⁷⁵ The Executive Branch agencies advise that “[t]he Chinese government’s controls over the Parent Entity [China Telecom Corporation Limited] and [China Telecom Americas], combined with newly enacted Chinese laws, raise significant concerns that [China Telecom Americas] will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests.”⁷⁶ These new laws include the Cybersecurity Law of the People’s Republic of China, effective June 1, 2017,⁷⁷ and the implementing regulation for the Cybersecurity Law, effective November 1, 2018.⁷⁸ Indeed, the former U.S. National Security Advisor has recently cautioned about “the integrated nature of the Chinese Communist Party’s military and economic strategies,” noting that the Chinese Communist Party “is obsessed with control—both internally and externally,” and that under Article 7 of China’s National Intelligence Law, “all Chinese companies must collaborate in gathering intelligence.”⁷⁹ Based on the record evidence, the Executive Branch agencies have made a serious and compelling case that China Telecom Americas’ use of its domestic and international section 214 authorizations poses a national security risk and also raises substantial law enforcement concerns, which China Telecom Americas has failed to adequately refute thus far.

23. The record evidence supports the concern raised by the Executive Branch agencies with respect to changes to China Telecom Corporation Limited’s Articles of Association,⁸⁰ that these

⁷⁵ *Id.* at 36 (citing *id.*, Exh. 48 at EB-735 and EB-766, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018; *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).

⁷⁶ *Id.* at 38.

⁷⁷ The 2017 Cybersecurity Law requires that telecom and network operators cooperate extensively with the Chinese government. *Id.* at 38-39; *see also id.*, Exh. 4 at EB-86, China Telecom Corp. Ltd., Annual Report Form 20-F (Apr. 27, 2018). 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.” *Id.*, Exh. 51 at EB-866, Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017), <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>.

⁷⁸ *Id.* at 38. The 2018 Regulation on Internet Security Supervision by Public Security Organs (2018 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 to ensure compliance with the inspection or, for remote inspections, the use of certain cybersecurity service agencies. *Id.* at 39-40 (citing *id.*, Exh. 54 at EB-904, EB-905, EB-907, EB-909, 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/>).

⁷⁹ H.R. McMaster, *What China Wants*, The Atlantic, May 2020, at 70, 71, 72-73 (*What China Wants*). *See also* H.R. McMaster, *How China Sees the World: And How We Should See China* (May 2020), <https://www.theatlantic.com/magazine/archive/2020/05/mcmaster-china-strategy/609088/>.

⁸⁰ *See* Executive Branch Recommendation to Revoke and Terminate at 36; *id.*, Exh. 48 at EB-735, EB-766, China Telecom Corp. Ltd., Annual Report (Form 20-F) (Apr. 27, 2018), Ex. 1.1 (Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018); *id.*, Exh. 114 at EB-2404, Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress, Article 33 (Oct. 24, 2017), http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf (Revised Constitution of the Communist Party of China). Article 33 of the Revised Constitution of the Communist Party of China states, among other things, that “[t]he leading Party members groups or Party committees of state-owned enterprises shall play a leadership role, set the right direction, keep in mind the big picture, ensure the implementation of Party policies and principles, and discuss and decide on major issues of their enterprise in accordance with regulations.” *Id.*, Exh. 114 at EB-2404. Article 33 further states that “[p]rimary-level Party organizations in state-owned or collective enterprises should

(continued....)

amendments signify the Chinese government’s ability to influence state-owned enterprises, and consequently their indirect subsidiaries.⁸¹ Additionally, China Telecom Americas’ corporate governance information shows that the current officers and directors of China Telecom Corporation Limited who are not {[]} and all current officers and directors of China Telecom are {[]}.⁸² The record shows that three of the individuals who are identified as a {[]} of China Telecom Americas’ Board of Directors are {[]}.⁸³ China Telecom Americas fails to provide evidence to rebut these concerns. Moreover, China Telecom Americas provides no supporting evidence for its argument that the changes to the Articles of Association were made to improve corporate governance and does not dispute that the amendments to China Telecom Corporation Limited’s Articles of Association confer express powers to Chinese Communist Party organizations within China Telecom Corporation Limited.⁸⁴ In fact, the language clearly details the responsibilities to the Chinese government and how involved the Chinese government is with respect to business operations, such as decisions and hiring. For example, Article 9 of China Telecom Corporation Limited’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.”⁸⁵ Moreover, Article 98 of China Telecom Corporation Limited’s amended Articles of Association states that, “[p]rior to making decisions on material issues of the Company, the board of

(Continued from previous page) _____

focus their work on the operations of their enterprise. Primary-level Party organizations shall guarantee and oversee the implementation of the principles and policies of the Party and the state within their own enterprise and shall support the board of shareholders, board of directors, board of supervisors, and manager (or factory director) in exercising their functions and powers in accordance with the law.” *Id.* Article 32 states that “[p]rimary-level Party organizations play a key role for the Party in the basic units of social organization” and that their “main tasks” include “to encourage Party members and the people to consciously resist unacceptable practices and resolutely fight against all violations of Party discipline or state law.” *Id.* at EB-2403-04.

⁸¹ *Id.* at 35-36; *id.*, Exh. 116 at EB-2566-2568, U.S. Trade Representative, 2018 Report to Congress on China’s WTO Compliance (Feb. 2019) (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”); *id.*, Exh. 60 at EB-1066, Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974, Office of the U.S. Trade Representative, <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF> (Mar. 22, 2018) (discussing that, “[t]hrough the [Chinese Communist Party], the Chinese government exercises additional control over [state-owned enterprise] behavior”); 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) (stating 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”).

⁸² China Telecom Americas Response, Exh. 5.

⁸³ *Id.*, Exh. 4.

⁸⁴ China Telecom Americas 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.” China Telecom Americas Response, Exh. 15 at 6.

⁸⁵ Executive Branch Recommendation to Revoke and Terminate, Exh. 48 at EB-735, China Telecom Corp. Ltd., Annual Report (Form 20-F) (Apr. 27, 2018), Ex. 1.1 (Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018).

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.”⁸⁶

24. With respect to the 2017 Cybersecurity Law cited by the Executive Branch agencies, China Telecom Americas does not dispute that it gives the Chinese government authority over the operations of its parent entities. Instead, China Telecom Americas argues that “Team Telecom vastly overstates the risks associated with [China Telecom Americas’] U.S. Records given the actual content and locations of those records”⁸⁷ and that the laws “are taken out of context, to suggest that relevant government authorities in China will have unrestricted powers in requesting information or extensive cooperation from [China Telecom Americas].”⁸⁸ China Telecom Americas states that the 2017 Cybersecurity Law “gives the Chinese government no authority over [China Telecom Americas’] operations in the United States.”⁸⁹ China Telecom Americas argues that the 2018 Regulation “was formulated and promulgated according to the Cybersecurity Law and the Police Law of the People’s Republic of China” and that those laws “are applicable only within the territory of China.”⁹⁰ China Telecom Americas also states that it “entered into an arms-length Records Security Agreement with [China Telecom Corporation Limited] expressly for, among other things, the purpose of ensuring compliance with the LOA.”⁹¹

25. Contrary to China Telecom Americas’ arguments and the Records Security Agreement with China Telecom Corporation Limited, the record shows that the Executive Branch agencies identified national security risks that are no longer theoretical.⁹² The Executive Branch agencies observe that {[

⁸⁶ *Id.* at EB-766.

⁸⁷ China Telecom Americas Response, Exh. 16 at 29. China Telecom Americas contends that “the types of information that [China Telecom Americas] 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.*

⁸⁸ *Id.* at 55.

⁸⁹ *Id.* at 56.

⁹⁰ *Id.*

⁹¹ *Id.* at 52 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-621, EB-625-26); *see* Executive Branch Recommendation to Revoke and Terminate at 18 & n.64 (citing *id.*, Business Confidential Exh. 36 at EB-621, Dec. 6, 2018 Letter from Morgan Lewis to DOJ National Security Division with attachments. The Executive Branch agencies state that China Telecom Americas provided a {[

]} *Id.* (citing *id.*, Business Confidential Exh. 37 at EB-655, E-mail from Morgan Lewis to DOJ National Security Division (Jan. 24, 2019)).

⁹² According to the Executive Branch agencies, “[t]he Executive Branch’s concerns about these laws (*i.e.*, the level of access and the inability to challenge the laws) is no longer theoretical. [China Telecom Americas] has disclosed that, {[

]} Executive Branch Recommendation to Revoke and Terminate at 40. The Executive Branch agencies assert that {[

]} *Id.*

}}⁹⁵ The record evidence regarding China Telecom Americas’ corporate governance and the officers, directors, and senior management officials of China Telecom Americas and its parent entities further reinforces the national security and law enforcement concerns that the Executive Branch agencies have raised regarding the ownership and control of China Telecom Americas.⁹⁶ In light of this relationship and based on China Telecom Corporation Limited’s Articles of Association and Chinese law, China Telecom Americas is highly likely to be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight.⁹⁷

26. Among various arguments, China Telecom Americas states that “[a]lthough [it] is owned by a corporation that is incorporated in China, [China Telecom Americas] is not subject or vulnerable to the ‘exploitation, influence, and control’ of the Chinese government in the way alleged by the Executive Branch agencies in their Recommendation.”⁹⁸ China Telecom Americas states that it “is a corporation

⁹³ *Id.* at 37-38 (citing *id.*, Business Confidential Exh. 36 at EB-621). {{

}} *Id.*, Business Confidential Exh. 36 at EB-621; *see id.* at 38 (citing *id.*, Business Confidential Exh. 36 at EB-621).

⁹⁴ *Id.* at 22 (referring to *id.*, Business Confidential Exh. 36 at EB-622, EB-623).

⁹⁵ *Id.* at 23. In particular, the Executive Branch agencies state that {{

}} *Id.* at 24 (citing *id.*, Business Confidential Exh. 103 at EB-2111, EB-2112, EB-2113, Apr. 4, 2019 Letter from Morgan Lewis to DOJ National Security Division; *id.* Business Confidential Exh. 36 at EB-622).

⁹⁶ *See generally* China Telecom Americas Response, Exhs. 3-5.

⁹⁷ The Executive Branch agencies assert that “[s]ome of the concerns raised by the Commission in [the *China Mobile USA Order*] about the Chinese government’s ability to influence state-owned enterprises, and consequently their indirect subsidiaries, may have already been realized when it comes to [China Telecom Americas].” Executive Branch Recommendation to Revoke and Terminate at 35. The Executive Branch agencies state that “in [the *China Mobile USA Order*], the Commission noted a [U.S. Trade Representative] report which stated that state-owned enterprises ‘are being pressured to amend their articles of association to ensure Communist Party representation on their boards of directors . . . and to ensure that they make important company decisions in consultation with internal Communist Party committees.’” *Id.* (quoting *China Mobile USA Order*, 34 FCC Rcd at 3370, para. 18, n.60).

⁹⁸ China Telecom Americas Response, Exh. 15 at 1. China Telecom Americas further asserts that its “shareholder [China Telecom Corporation Limited] is subject to rigorous legal regulation and public oversight, and must comply with the Company Law of the People’s Republic of China (‘PRC’), the rules and governance requirements in the HKEx Listing Rules, and the securities regulations in the U.S., including the rules on the appointment of independent directors, protection of minority shareholders and public information disclosure.” *Id.* at 2-3. China Telecom Americas also asserts that the State-owned Assets Supervision and Administration Commission of the State Council “does not have social or public management functions, and it is not in a position, nor does it have any mandate, to ‘exploit, influence or control’ [state-owned enterprises] (or their domestic and overseas subsidiaries).” *Id.* at 5. China Telecom Americas argues that “[a]s a corporation governed by the General Corporation Law of the State of Delaware, [China Telecom Americas] directors and management must discharge their fiduciary duties

(continued....)

organized and existing under the laws of the State of Delaware.”⁹⁹ China Telecom Americas contends that “[e]ssentially, the Recommendation asks the Commission to disregard [China Telecom Americas] existence as a separate corporate entity.”¹⁰⁰

27. In the *China Mobile USA Order*, we found unpersuasive a similar argument made by China Mobile USA.¹⁰¹ We noted 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.”¹⁰² Moreover, as we observed in the *Protecting Against National Security Threats Order*, “the Chinese government is highly centralized and exercises strong control over commercial entities, permitting the government, including state intelligence agencies, to demand that private communications sector entities cooperate with any governmental requests, which could involve revealing customer information, including network traffic information.”¹⁰³ We find China Telecom Americas’ argument that it is not subject to the control of the Chinese government because it is organized in the State of Delaware unpersuasive in light of the record and our findings in other proceedings. China Telecom Americas has thus far failed to adequately rebut the Executive Branch agencies’ demonstration of the substantial likelihood that China Telecom Americas would be forced to comply with Chinese government requests “without sufficient legal process or judicial oversight.”¹⁰⁴

28. China Telecom Americas asserts that it “is a profit-making, commercial enterprise that operates on a day-to-day basis independently and without interference from its parent company on core business matters”¹⁰⁵ However, China Telecom Americas also states that its “Bylaws authorize [China Telecom Corporation Limited], as the sole stockholder of [China Telecom Americas], to examine the Board’s reports, . . . approve and amend [China Telecom Americas]’ core institutional documents, and approve other major matters which are subject to the approval of stockholders” and that “[China Telecom Corporation Limited] may also authorize or delegate to the Board to carry out such matters.”¹⁰⁶ Three of the individuals identified as a {{ }} of China Telecom Americas’ Board of Directors are identified as {{

(Continued from previous page) _____

towards [China Telecom Corporation Limited], the sole shareholder of [China Telecom Americas], in a way that maximizes shareholder return on investment. However, the fiduciary duties owed are not without limits and the subsidiary may not act in a way contrary to applicable local law. None of the shareholders of [China Telecom Americas], whether direct or indirect, can instruct [China Telecom Americas] to do whatever the shareholder desires, and the company itself, its shareholders and directors/management must operate within the parameters of applicable law, conduct codes and articles of association.” *Id.* at 2.

⁹⁹ *Id.* at 1.

¹⁰⁰ *Id.*, Exh. 16 at 47.

¹⁰¹ *China Mobile USA Order*, 34 FCC Rcd at 3371, para. 19; *see 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.’”).

¹⁰² *Id.* at 3369, para. 17 (footnotes omitted).

¹⁰³ *Protecting Against National Security Threats Order*, 34 FCC Rcd at 11441, para. 46; *see also What China Wants* at 69-74.

¹⁰⁴ Executive Branch Recommendation to Revoke and Terminate at 37.

¹⁰⁵ China Telecom Americas Response, Exh. 3 at 1.

¹⁰⁶ *Id.* at 2.

¹⁰⁷ *Id.*, Exh. 4.

}}¹¹² Based on the record to date, we are unpersuaded by China Telecom Americas' argument that "[t]here is no rational link between [China Telecom Americas'] U.S. authorizations and the Chinese government's regulation of its parent company's operations in China."¹¹³

2. National Security and Law Enforcement Risks Associated with China Telecom Americas' Retention of Section 214 Authorities

29. Based on the record, we believe there are national security and law enforcement risks associated with China Telecom Americas' retention of its domestic section 214 authority and international section 214 authorizations.

30. The Executive Branch agencies assert that "[t]he national security environment has changed significantly since 2007, when the Commission last certified [China Telecom Americas'] international Section 214 authorizations to provide international common carrier services."¹¹⁴ The Executive Branch agencies advise that in recent years, the U.S. government has been concerned about the

¹⁰⁸ Executive Branch Recommendation to Revoke and Terminate, Exh. 4 at EB-63, EB-67, China Telecom Corp. Ltd., Annual Report Form 20-F (Apr. 27, 2018). In its October 1, 2018 response to the Executive Branch agencies' inquiry, China Telecom Americas stated that {

}} *Id.*, Business Confidential Exh. 92 at EB-1983, EB-1985. {{

}} *Id.* at EB-1985.

{{

}} *Id.*, Business Confidential Exh. 36

at EB-640.

¹⁰⁹ China Telecom Americas Response, Exh. 5. Based on the record, {{ }} individuals identified as the current officers and directors of CTCL (including all individuals identified as an officer and/or {{

}} *Id.*

¹¹⁰ China Telecom Americas Response, Exhs. 1-1, 2; *see also* Executive Branch Recommendation to Revoke and Terminate at 32-33.

¹¹¹ China Telecom Americas Response, Exh. 5 at 1, 7.

¹¹² *Id.* at 1-2, 8.

¹¹³ *Id.*, Exh. 16 at 57.

¹¹⁴ Executive Branch Recommendation to Revoke and Terminate at 2; *see also id.* at 2-7. The Executive Branch agencies assert that "[i]n 2007, the U.S. Intelligence Community's top concern was terrorism, with the countries of highest concern being Iraq, Afghanistan, and Pakistan," and 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." *Id.* 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)).

Chinese government's malicious cyber activities. The agencies cite to the 2019 Office of the Director of National Intelligence worldwide threat assessment, in which "China is the first country identified by name for its persistent economic espionage and growing threat to core military and critical infrastructure systems."¹¹⁵ The Executive Branch agencies state that "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."¹¹⁶

31. The Executive Branch agencies state that "[China Telecom Americas'] U.S. operations provide opportunities for Chinese state-sponsored actors to engage in espionage, to steal trade secrets and other confidential business information, and to disrupt and misroute U.S. communications traffic."¹¹⁷ The Executive Branch agencies advise that China Telecom Americas' "status as a managed services provider (MSP) provides abundant opportunities for Chinese government-sponsored actors, as described in a recent federal indictment."¹¹⁸ The Executive Branch agencies also state that "[China Telecom Americas'] managed network and security services similarly provide opportunities for Chinese government-sponsored cyber actors" and cite a 2018 federal indictment.¹¹⁹ The Executive Branch agencies assert that China Telecom Americas' "access to its clients' U.S. records may provide additional opportunities for Chinese government-sponsored cyber actors" and that "[c]oncerns about such access are heightened by prior reporting that [China Telecom Americas'] Chinese affiliates have aided the Chinese government's economic espionage efforts."¹²⁰ In addition, the Executive Branch agencies refer to public reports that China Telecom Americas' network misrouted large amounts of information and communications traffic, over long periods of time, often several months,¹²¹ sometimes involving U.S. government traffic.¹²² The

¹¹⁵ *Id.* at 2 (citing *id.*, Exh. 8 at EB-351, *Worldwide Threat Assessment of the U.S. Intelligence Community Before the S. Select Comm. On Intelligence*, 116th Cong. 5 (2019) (statement of Daniel R. Coats, Director of National Intelligence)). Moreover, the Executive Branch agencies state that "[t]he [Office of the Director of National Intelligence's] 2019 global threat assessment warns not only of the Chinese government's cyber activities but also of the potential use of 'Chinese information technology firms as routine and systemic espionage platforms against the United States and allies.'" *Id.* at 3 (citing *id.*, Exh. 8 at EB-351) (emphasis added).

¹¹⁶ *Id.* at 6 (citing *id.*, Exh. 61 at EB-1205-17, Office of the U.S. Trade Representative, *Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation*, at 10-22 (Nov. 20, 2018), <https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf>).

¹¹⁷ *Id.* at 41. The Executive Branch agencies explain that "the Executive Branch has in the past year escalated its warnings about the threats posed by Chinese government-sponsored cyber actors in the current national security environment. These warnings are not limited to direct acts by 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." *Id.* (citing *id.*, Exh. 8 at EB-351).

¹¹⁸ *Id.* at 42.

¹¹⁹ *Id.* (citing *id.*, Exh. 98 at EB-2034, *United States v. Zhang*, No. 13-cr-3132, Indictment (S.D. Cal. Oct. 25, 2018)).

¹²⁰ *Id.* at 43.

¹²¹ China Telecom Americas argues that "in reality, internet routing problems are common and occur on all networks despite the best efforts of responsible operators." China Telecom Americas Response, Exh. 16 at 61. Its argument, however, simply ignores the important role played by service providers in lessening the impacts of such routing issues. 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 [China Telecom Americas]. For nearly a decade, [China Telecom Americas] has been on notice that its network advertised incorrect routing information to its neighbors on the Internet."); *id.* at 49 ("In today's national security environment, [China Telecom Americas'] access to the U.S. communications network, [] creates a vulnerability that is just as real as failing to monitor flammable fumes on a factory floor. [China Telecom Americas'] U.S. operations present opportunities, and plausible deniability, for Chinese state-sponsored actors to disrupt and misroute U.S. Internet traffic.").

Executive Branch agencies further argue that “[China Telecom Americas’] U.S. presence also allows China to disrupt U.S. Internet traffic for political purposes.”¹²³

32. China Telecom Americas has thus far not persuaded us that its section 214 authorizations do not provide China Telecom Americas opportunities for economic espionage against U.S. targets given the totality of the evidence in the record.¹²⁴ China Telecom Americas states that its “business model, including its access to customer data, does not provide what the Recommendation suggests as opportunities for economic espionage.”¹²⁵ China Telecom Americas argues 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.”¹²⁶

33. Contrary to China Telecom Americas’ argument, collection and maintenance of records pertaining to the provision and billing for services do not comprise the sole means by which China Telecom Americas, or any other service provider, can collect records about its customers. A service provider, such as China Telecom Americas, could analyze application content or metadata derived from packets transiting a device or infrastructure that is managed by the service provider. For example, tools that are used by a service provider to identify network intrusion¹²⁷ or perform deep packet inspection can

(Continued from previous page)

¹²² Executive Branch Recommendation to Revoke and Terminate at 45. The Executive Branch agencies identify 10 examples of such reported incidents. *See id.* at 45-47. The Executive Branch agencies state that “[w]hen asked to explain, [China Telecom Americas] 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).

¹²³ *Id.* at 50. The Executive Branch agencies refer to “[China Telecom Americas’] seeming involvement in the ‘Great Cannon’ denial of service attacks” when, according to an April 2015 paper published by the University of Toronto’s Citizen Lab, “[China Telecom Americas’] network was used to insert malicious code onto computers in the United States visiting Chinese sites. The computers were then reportedly co-opted to carry out the ‘Great Cannon’ distributed denial of service attack on GitHub and GreatFire.org.” *Id.* at 50-51 (citing *id.*, Exh. 104 at EB-2119, B. Marczak et al, *Research Brief, China’s Great Cannon*, The Citizen Lab (Apr. 2015), <https://citizenlab.ca/wp-content/uploads/2009/10/ChinasGreatCannon.pdf>; *id.*, Exh. 105 at EB-2134, J. Griffiths, *When Chinese hackers declared war on the rest of us*, MIT Technology Review (Jan. 10, 2019), <https://www.technologyreview.com/2019/01/10/103560/when-chinese-hackers-declared-war-on-the-rest-of-us/>). The Executive Branch agencies contend that “[t]he Great Cannon attack specifically targeted materials on GitHub and GreatFire that provided technologies for users who wished to circumvent Chinese government censorship, including the Chinese-language version of the New York Times.” *Id.* at 51 (citing *id.*, Exh. 104 at EB-2123; *id.*, Exh. 105 at EB-2135).

¹²⁴ China Telecom Americas Response, Exh. 16 at 57-58.

¹²⁵ *Id.* at 57.

¹²⁶ *Id.* at 58.

¹²⁷ *See, e.g.*, 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 Detection and Prevention Systems). 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>.

be leveraged by such service provider to perform “pervasive monitoring,” which has been identified as “an attack on the privacy of Internet users and organizations.”¹²⁸ Moreover, while it may be true that the records China Telecom Americas 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 China Telecom Americas is now required to operate.

34. China Telecom Americas also fails to dispute the Executive Branch agencies’ argument that China Telecom Americas’ Managed Service Provider offering could provide abundant opportunities for unauthorized access to data.¹²⁹ China Telecom Americas claims that its “[Managed Service Provider] service—[‘]NetCare’—only monitors connectivity and transmission quality on the [China Telecom Americas]-provided circuit, and does not have access to any customer-owned equipment unless the customer authorizes that access for trouble-shooting purposes.”¹³⁰ We understand that China Telecom Americas, like any other service provider, only has access to equipment and systems of its customers if authorized by those customers, and we note that unauthorized access would potentially be a violation of federal law in the United States.¹³¹ As an initial matter, we understand that it is normal practice for service providers to request and receive authorization to access customers’ equipment and systems to monitor quality of service, and that the value of a monitoring service with no such access is limited. At the same time, China Telecom Americas has the technical ability, with or without the authorization of its customers, to observe, gather, intercept, inspect, and alter or compromise data that transit its network or any equipment under its management.¹³² China Telecom Americas also states that it offers “Multiple Protocol Label Switching/Virtual Private Network” (MPLS/VPN) service, which “provides customers

¹²⁸ See Internet Engineering Task Force (IETF), *Request For Comments: 7258, Category: Best Current Practice, Pervasive Monitoring is an Attack* (May 2014), <https://www.rfc-editor.org/rfc/rfc7258.txt>.

¹²⁹ Executive Branch Recommendation to Revoke and Terminate at 41-43.

¹³⁰ China Telecom Americas Response, Exh. 16 at 58.

¹³¹ See, e.g., Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030; Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510. Allowing unauthorized access to Customer Proprietary Network Information (CPNI) is a violation of section 222 of the Act as well as Commission rules implementing section 222. See 47 U.S.C. § 222; 47 CFR §§ 64.2001-2011. Further, the Executive Branch agencies state that China Telecom Americas {

} See Executive Branch Recommendation to Revoke and Terminate at 27.

¹³² Monitoring network traffic provides access to sensitive information for multiple purposes. This is true whether the traffic is encrypted or not. See, e.g., NIST Guide to Intrusion Detection and Prevention Systems (discussing network based detection, wireless detection, and analysis of network traffic); Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, National Institute of Standards and Technology (NIST), *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86 (2006), <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf> (discussing use of data from network traffic, network traffic data sources, collecting network traffic data, and examining and analyzing traffic data); Paul Cichonski, Tom Millar, Tim Grance & Karen Scarfone, *Computer Security Incident Handling Guide*, NIST Special Publication 800-61 Revision 2 (2012), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> (generally discussing detection and analysis of data). Recent research analyzes specific scenarios and further outlines how traffic can be monitored. See, e.g., Monica Skowron, Artur Janicki & Wojciech Mazurczyk, *Traffic Fingerprinting Attacks on Internet of Things Using Machine Learning* (IEEE Access: Vol. 8, at 20386-20400) (2020), <http://doi.org/10.1109/ACCESS.2020.2969015>; Noah Apthorpe, Danny Yuxing Huang, Dillon Reisman, Arvind Narayanan, & Nick Feamster, *Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping* (Proceedings on Privacy Enhancing Technologies: Vol. 2019, Issue 3, at 128-148) (2019), <https://doi.org/10.2478/popets-2019-0040>; Jan Kohout & Tomáš Pevný, *Network Traffic Fingerprinting Based on Approximated Kernel Two-Sample Test* (IEEE Transactions on Information Forensics and Security: Vol. 13, Issue 3, at 788-801) (2018), <http://doi.org/10.1109/TIFS.2017.2768018>.

with highly secured data transmission for logical connectivity among multiple destinations,”¹³³ and that “[China Telecom Americas] offers Internet Protocol Security (‘IP Sec’) VPN service, which allows a site to communicate with other MPLS VPN sites with Internet connectivity through IP Sec tunnels.”¹³⁴ These are not end-to-end services from a user’s source device (e.g., laptop, desktop, smart phone) to a destination device outside of a service provider’s network, but are services offered at the ingress, or within, the company’s network. For these types of service offerings, China Telecom Americas has access to data (i.e., metadata and any unencrypted application content) as data enter and exit its network.¹³⁵ As experts testify, a 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.”¹³⁶

35. Even if, for any reason, China Telecom Americas 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 potentially be used for espionage. While such practices are true for virtually all service providers, other such providers are not identified like China Telecom Americas as posing a national security and law enforcement risk. Such concerns have been raised recently by the Executive Branch agencies.¹³⁷ The Executive Branch agencies state that “[i]n August 2018, [DOD] warned that ‘China uses its cyber capabilities to support intelligence collection against U.S. diplomatic, economic, academic, and defense industrial base sectors.’”¹³⁸ The Executive Branch agencies further state that “[i]n December 2018, DHS stated that ‘[n]ation-state actors such as China . . . have used cyber intrusions to steal private sector proprietary information and sabotage military and critical infrastructure. [] China will continue to use cyber espionage and bolster cyber attack capabilities to support its national security priorities.’”¹³⁹ In

¹³³ China Telecom Americas Response, Exh. 6 at 4.

¹³⁴ *Id.* MPLS/VPN is a suite of protocols that encapsulates packets with an MPLS defined header and forwards the traffic through a virtual private network. See Internet Engineering Task Force (IETF), *Request For Comments: 3031, Category: Standards Track, Multiprotocol Label Switching Architecture* (Jan. 2001), <https://tools.ietf.org/html/rfc3031>. Using MPLS headers facilitates very fast forwarding of traffic. *Id.* at 4-6, Section 2.1. IPsec uses an IP header to encapsulate an IP packet and either encrypt the payload or insert a digital signature to support integrity. Internet Engineering Task Force (IETF), *Request For Comments: 4301, Category: Standards Track, Security Architecture for the Internet Protocol* at 6-9-10, Section 3.2 (Dec. 2005), <https://tools.ietf.org/html/rfc4301>.

¹³⁵ See Internet Engineering Task Force (IETF), *Request For Comments: 3031, Category: Standards Track, Multiprotocol Label Switching Architecture* (Jan. 2001), <https://tools.ietf.org/html/rfc3031>; Internet Engineering Task Force (IETF), *Request For Comments: 6178, Category: Standards Track, Label Edge Router Forwarding of IPv4 Option Packets* (Mar. 2011), <https://tools.ietf.org/html/rfc6178>.

¹³⁶ See Letter from Paul Ohm, Professor of Law, Georgetown University Law Center and Faculty Director, Georgetown Center on Privacy and Technology, to Marlene H. Dortch, Secretary, FCC, WC Docket No. 16-106, Attach. at 3 (filed June 20, 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); see also NIST Guide to Intrusion Detection and Prevention Systems (discussion on Deep Packet Inspection).

¹³⁷ Executive Branch Recommendation to Revoke and Terminate at 3.

¹³⁸ *Id.* (citing *id.*, Exh. 65 at EB-1384, Office of the Sec’y of Def. Ann. Rep. to Cong., *Military and Security Developments Involving the People’s Republic of China 2018*, at 75 (Aug. 16, 2018), <https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/2018-CHINA-MILITARY-POWER-REPORT.PDF>).

¹³⁹ *Id.* (citing *id.*, Exh. 59 at EB-973, *China’s Non-traditional Espionage Against the United States: The Threat and Potential Policy Responses: Hearing Before the S. Comm. on the Judiciary*, 115th Cong., at 1 (Dec. 12, 2018) (statement of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security)).

addition, the Executive Branch agencies state that “[i]n November 2018, the Director of the Federal Bureau of Investigation (FBI) warned that ‘no country poses a broader, more severe intelligence collection threat than China. [] Nearly every FBI field office currently has economic espionage cases that lead back to China’”¹⁴⁰ The Executive Branch agencies assert that “[b]y the end of 2018, DOJ had announced multiple indictments of Chinese state actors targeting the U.S. private sector.”¹⁴¹ As General McMaster has concluded, “Chinese cybertheft is responsible for what General Keith Alexander, the former director of the National Security Agency, described as the ‘greatest transfer of wealth in history.’”¹⁴² We view the arguments of the Executive Branch agencies and other experts regarding these matters as persuasive and give weight to their expertise as they raise significant concerns regarding the risks associated with China Telecom Americas’ section 214 authorizations.

36. China Telecom Americas states that while the Executive Branch agencies argue that “‘the national security environment has changed significantly since 2007,’” the U.S. government’s concerns about the Government of China do not relate “directly to [China Telecom Americas] or even to its corporate parent and affiliates.”¹⁴³ The heightened national security and law enforcement risks were previously identified by the Executive Branch agencies in their recommendation to deny China Mobile USA’s application for an international section 214 authorization.¹⁴⁴ In the *China Mobile USA Order*, we denied China Mobile USA’s application and determined that China Mobile USA, like China Telecom Americas, is ultimately owned and controlled by the Chinese government.¹⁴⁵ We stated that “in the current security environment, there is a significant risk that the Chinese government would use the grant of such authority to China Mobile USA to conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States.”¹⁴⁶ In that case, we recognized that “the Executive Branch agencies identify significantly enhanced national security and law enforcement risks linked to the Chinese government’s activities since the Commission last granted international section 214 authorizations to other Chinese state-owned companies more than a decade ago.”¹⁴⁷ Based on the record, China Telecom Americas’ “ongoing operations in the United States raise similar—but more pressing—national security and law enforcement concerns,” as indicated by the Executive Branch agencies.¹⁴⁸ In light of China Telecom Americas’ relationship to the Chinese Communist Party and the Chinese government as well as the Chinese law that China Telecom Americas and its direct and indirect parent

¹⁴⁰ *Id.* at 4 (citing *id.*, Exhibit 90 at EB-1971, Christopher Wray, Dir. Fed. Bureau of Investigation, Address at the Ninth Annual Financial Crimes and Cybersecurity Symposium, Keeping our Financial Systems Secure: a Whole-of-Society Approach, at 2 (Nov. 1, 2018), <https://www.fbi.gov/news/speeches/keeping-our-financial-systems-secure-a-whole-of-society-response>).

¹⁴¹ *Id.*

¹⁴² *What China Wants* at 73.

¹⁴³ China Telecom Americas Response, Exh. 16 at 17-18. China Telecom Americas argues that “the Commission should not revoke any authorizations held by [China Telecom Americas] based on the state of international relations between the United States and China, but only (if at all) based on facts and conduct specifically related to [China Telecom Americas].” *Id.* at 18.

¹⁴⁴ See *China Mobile USA Order*, 34 FCC Red at 3368-77, paras. 14-33; Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.’s Application for an International Section 214 Authorization, File No. ITC-214-20110901-00289 at 7-17 (filed July 2, 2018).

¹⁴⁵ *China Mobile USA Order*, 34 FCC Red at 3363, 3365-66, paras. 3, 8.

¹⁴⁶ *Id.* at 3365-66, para. 8.

¹⁴⁷ *Id.* at 3371-72, para. 20.

¹⁴⁸ Executive Branch Recommendation to Revoke and Terminate at 15.

entities and affiliates must adhere to, the evidence in the record does not support China Telecom Americas' arguments.

3. China Telecom Americas' Past Conduct and Representations to the Executive Branch Agencies

37. China Telecom Americas' past conduct and representations to the Executive Branch agencies raise concerns regarding whether China Telecom Americas should retain its domestic section 214 authority and international section 214 authorizations. The Executive Branch agencies assert that "Team Telecom, while monitoring [China Telecom Americas'] LOA compliance over the past year, has discovered conduct that calls into question [China Telecom Americas'] trustworthiness."¹⁴⁹ The Executive Branch agencies contend that this conduct "includes [China Telecom Americas'] delayed responses to Team Telecom requests for information, its inaccurate statements to Team Telecom and U.S. customers, and its apparent failure to comply" with federal law.¹⁵⁰ The Executive Branch agencies advise that China Telecom Americas "delayed six months before providing documents in response to a Team Telecom request. This calls into question its willingness to cooperate with Team Telecom to monitor compliance with the LOA."¹⁵¹ Moreover, the Executive Branch agencies state that "[a]side from the delays, the Executive Branch is troubled by new disclosures in these documents that indicate [China Telecom Americas] made inaccurate statements to U.S. government authorities about where it stored U.S. records and to U.S. customers about its cybersecurity practices."¹⁵²

38. The Executive Branch agencies state that in 2019, the agencies made an inquiry to China Telecom Americas about {[

]}¹⁵³ After further questioning by the Executive Branch agencies, China Telecom Americas admitted that {[

]}¹⁵⁴ The Executive Branch agencies argue that this admission contradicts a statement made by China Telecom Americas in January 2016 "that {[]}¹⁵⁵ The Executive Branch agencies state that China Telecom Americas previously represented to the Executive Branch agencies that {[

]}¹⁵⁶ These inconsistencies are even more troubling in view of {[

¹⁴⁹ *Id.* at 17.

¹⁵⁰ *Id.*

¹⁵¹ *Id.*

¹⁵² *Id.* at 18-19.

¹⁵³ *Id.* at 19 (citing *id.*, Business Confidential Exh. 36 at EB-624); *see also id.* at 25; *id.*, Business Confidential Exh. 96 at EB-2000-2003, Mar. 21, 2019 Letter from DOJ National Security Division to Morgan Lewis; *id.*, Business Confidential Exh. 102 at EB-2103-06, Mar. 21, 2019 Letter from DOJ National Security Division to Morgan Lewis.

¹⁵⁴ *Id.* at 19.

¹⁵⁵ *Id.*

¹⁵⁶ *Id.* at 19-20. Additionally, the Executive Branch agencies state that {[

]} *Id.*

}}¹⁵⁷

39. The Executive Branch agencies' allegations concerning China Telecom Americas' lack of transparency and unwillingness to fully cooperate with the Executive Branch agencies appear to be true, especially with regard to the location of and access to its U.S. records. China Telecom Americas argues that its statements to the Executive Branch agencies concerning its U.S. records "were accurate at the times the statements were made, and there were no contradictions or misrepresentations to Team Telecom"¹⁵⁸ and that "[t]he Recommendation is based on a misinterpretation of [China Telecom Americas'] statements about storage of and access to U.S. Records."¹⁵⁹ China Telecom Americas contends, for example, that there was no contradiction when it stated in one correspondence to the Executive Branch agencies that its U.S. records "were kept" at a location in the United States while it stated in a subsequent correspondence that the U.S. records "were available" to its non-U.S. affiliates outside of the United States.¹⁶⁰ According to China Telecom Americas, "[e]lectronic records can be 'kept' at one location and simultaneously be 'available' in other locations."¹⁶¹ However, it appears that China Telecom Americas was not transparent in its interactions with the Executive Branch agencies, {{

}}¹⁶² Given the Executive Branch agencies' role in protecting the security of the United States and the record evidence supporting the concerns that are raised because of the ultimate foreign ownership of China Telecom Americas, we give weight to the Executive Branch agencies' view that China Telecom Americas was not transparent, and likely failed to fully cooperate with a U.S. government agency.

40. Further, additional record evidence raises serious concerns regarding China Telecom Americas' interactions with the Executive Branch agencies during the course of their mitigation monitoring. As an initial matter, {{

¹⁵⁷ *Id.*, Business Confidential Exh. 3 at EB-15.

¹⁵⁸ China Telecom Americas Response, Exh. 16 at 20-21.

¹⁵⁹ *Id.* at 20.

¹⁶⁰ *Id.* at 21.

¹⁶¹ *Id.* China Telecom Americas further states that "[China Telecom Americas'] overseas affiliates have *always* had access to records about [China Telecom Americas'] U.S. services in some form, because that information is necessary for the affiliates to provision international circuits used to serve U.S. customers" and that "although [China Telecom Americas] was not under any formal obligation to do so under the LOA, [China Telecom Americas] did inform Team Telecom on at least two occasions before April 2019 that access was being provided to [China Telecom Americas] affiliates." *Id.* at 22.

¹⁶² See Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15.

¹⁶³ *Id.*, Business Confidential Exh. 32 at EB-576.

¹⁶⁴ *Id.*, Business Confidential Exh. 92 at EB-1983-85. {{

}} *Id.*, Business
(continued....)

}]¹⁶⁹ Importantly, compliance with the terms of the mitigation agreement is an express condition of the International Bureau’s grant of the *pro forma* transfer of control of China Telecom Americas’ international section 214 authorizations, and as discussed below, we similarly find the Executive Branch agencies’ arguments on this issue persuasive.¹⁷⁰

41. For these reasons, the Executive Branch agencies state that they “believe that [China Telecom Americas’] lack of trustworthiness and vulnerability to Chinese government exploitation, influence, and control would limit their ability to conduct statutorily authorized law enforcement and national security missions.”¹⁷¹ They also state that “[t]he U.S. government would not be able to work effectively with [China Telecom Americas] to identify and disrupt unlawful activities or to assist in investigating unlawful conduct as the U.S. government currently does with trusted communications providers. These efforts rely on a baseline level of trust between the government and telecommunications carriers.”¹⁷² The Executive Branch agencies also advise that “[b]ecause [China Telecom Americas] is ultimately owned by the Chinese government, the U.S. government cannot trust [China Telecom

(Continued from previous page) _____
Confidential Exh. 34, EB-581-83. {[

]} *Id.* at EB-581.

¹⁶⁵ *Id.*, Business Confidential Exh. 35 at EB-586-87.

¹⁶⁶ *Id.* at EB-586.

¹⁶⁷ *Id.*

¹⁶⁸ *Id.*, Business Confidential Exh. 36 at EB-589-654. The Executive Branch agencies argue that “[i]n response to a Team Telecom request for cybersecurity policies, [China Telecom Americas] delayed for six months before it provided an improperly redacted {[]} document.” *Id.* at 56. The Executive Branch agencies state that “[w]hen the redaction was finally removed, [China Telecom Americas’] underlying motivation could not have been more clear: [China Telecom Americas] wished {[

]} *Id.* (quoting *id.*,

Business Confidential Exh. 37 at EB-655).

¹⁶⁹ China Telecom Americas states that the Information Security Policy was an effort to “memorialize numerous cybersecurity and privacy policies already implemented by [China Telecom Americas].” China Telecom Americas Response, Exh. 16 at 39; *see also infra* para. 52.

¹⁷⁰ *See infra* paras. 51-52.

¹⁷¹ Executive Branch Recommendation to Revoke and Terminate at 51.

¹⁷² *Id.* at 51-52.

Americas] to identify, disrupt, or provide assistance for investigations into unlawful activity sponsored by the Chinese government.”¹⁷³

42. We similarly question China Telecom Americas’ transparency and whether China Telecom Americas can be relied upon to comply with our rules and procedures. First, China Telecom Americas does not dispute that it did not notify the Executive Branch agencies of its applications for ISPC assignments, as contemplated by the mitigation agreement, compliance with which is an express condition of the International Bureau’s grant of the *pro forma* transfer of control of its international section 214 authorizations.¹⁷⁴ Second, China Telecom Americas disregarded its responsibilities to the Commission as a holder of ISPCs. On November 18, 2020, based on information that China Telecom Americas filed in response to the *Order to Show Cause*, the International Bureau found that China Telecom Americas is not in compliance with the conditions of its provisional ISPC assignments, and reclaimed the three ISPCs.¹⁷⁵ Specifically, China Telecom Americas 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” and which China Telecom Americas had prior knowledge of and even certified to in its ISPC applications.¹⁷⁶ China Telecom Americas, for example, does not even cite to the Commission’s requirements in its response seeking to retain its ISPC assignments and nevertheless simply disregarded our requirements.¹⁷⁷

43. Overall, the record presents a troubling picture of China Telecom Americas’ lack of forthrightness in its responses to the Executive Branch agencies’ mitigation monitoring. We are unpersuaded by China Telecom Americas’ contention that its “conduct to date does not demonstrate any reasonable basis for the U.S. government’s stated lack of trust.”¹⁷⁸ As described above, the Executive Branch agencies have identified a number of instances where China Telecom Americas has not been transparent with and likely failed to fully cooperate with the Executive Branch agencies. Thus, based on the record evidence, we question China Telecom Americas’ transparency and reliability, qualities that are necessary for the public interest to support its continued holding of section 214 authority.

4. The Executive Branch Agencies Do Not Recommend Further Mitigation

44. The record concerning China Telecom Americas’ representations to the Executive Branch agencies, combined with the national security and law enforcement risks that the Executive Branch agencies identified with regard to China Telecom Americas’ vulnerability to the exploitation, influence, and control of the Chinese government, raises serious concerns as to whether the identified risks can be mitigated. Based on the record, China Telecom Americas has not demonstrated thus far that it can be trusted to cooperate with the Executive Branch agencies in good faith or that the national security and law enforcement concerns associated with its domestic section 214 authority and international section 214 authorizations can be mitigated.

45. The Executive Branch agencies do not recommend further mitigation, “because the underlying foundation of trust that is needed for a mitigation agreement to adequately address national

¹⁷³ *Id.* at 52.

¹⁷⁴ China Telecom Americas 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.”); *see infra* paras. 55-59.

¹⁷⁵ *See* ISPC Reclamation Letter.

¹⁷⁶ *Id.* at 1-2, 4; China Telecom Americas Response, Exh. 9 at 2; *see* Response to ISPC Reclamation Letter.

¹⁷⁷ ISPC Reclamation Letter at 4; China Telecom Americas Response, Exh. 9 at 1-2.

¹⁷⁸ China Telecom Americas Response, Exh. 16 at 63.

security and law enforcement concerns is not present here.”¹⁷⁹ The Executive Branch agencies argue that “[China Telecom Americas] 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.”¹⁸⁰ The Executive Branch agencies contend that China Telecom Americas “has also demonstrated an unwillingness to cooperate with mitigation monitoring.”¹⁸¹ The Executive Branch agencies assert that “[d]espite regular compliance monitoring, the U.S. government can never have full visibility into all of a company’s activities and must rely on the private party to adhere rigorously and scrupulously to mitigation agreements and to self-report instances of non-compliance. The U.S. government cannot rely on [China Telecom Americas] to do so.”¹⁸²

46. China Telecom Americas argues that “the Administrative Procedure Act seems to require that the Commission give [China Telecom Americas] an opportunity to mitigate any risks that it might identify.”¹⁸³ China Telecom Americas argues that “[a]ssuming *arguendo* that there were grounds for the Commission to consider revocation of [China Telecom Americas’] authorization — although there are not . . . — it would first have to give [China Telecom Americas] an ‘opportunity to demonstrate or achieve compliance with all lawful requirements.’”¹⁸⁴ Based on the record thus far, it appears that the national security and law enforcement risks identified in the record cannot be mitigated. The proceeding that we institute today will afford China Telecom Americas an additional opportunity to present arguments and evidence regarding whether the Commission should revoke its domestic section 214 authority and revoke and/or terminate its international section 214 authorizations.

B. Termination of International Section 214 Authorizations

47. We next consider whether termination of China Telecom Americas’ international section 214 authorizations is warranted, separate and apart from revocation, based on China Telecom Americas’ compliance with the conditions in the International Bureau’s grant of the *pro forma* transfer of control of its international section 214 authorizations. 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.”¹⁸⁵ China Telecom Americas’ two international section 214 authorizations are conditioned on abiding by the commitments and undertakings contained in its 2007 LOA.¹⁸⁶ 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.”¹⁸⁷ Here, in light of the deference accorded to the Executive Branch agencies on these issues, compliance with the commitments contained in the 2007 LOA was a material condition of the International Bureau’s grant of the *pro forma*

¹⁷⁹ Executive Branch Recommendation to Revoke and Terminate at 53.

¹⁸⁰ *Id.*

¹⁸¹ *Id.* at 55.

¹⁸² *Id.* at 55-56.

¹⁸³ China Telecom Americas Response, Exh. 16 at 71.

¹⁸⁴ *Id.* (quoting 5 U.S.C. § 558(c)(2)).

¹⁸⁵ 47 U.S.C. § 214(c).

¹⁸⁶ *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, DA 07-3632, 22 FCC Rcd 15266, 15268 (IB 2007) (“[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] . . .”).

¹⁸⁷ 2007 LOA at 3.

transfer of control of the authorizations, and failure to comply with such commitments accordingly warrants consideration of termination of such authorizations.¹⁸⁸

48. Based on the record evidence, it appears that China Telecom Americas' two international section 214 authorizations, ITC-214-20010613-00346 and ITC-214-20020716-00371, which are conditioned on China Telecom Americas abiding by the commitments and undertakings contained in the 2007 LOA, should be terminated. China Telecom Americas apparently has failed to comply with the terms of the 2007 LOA and thus of the express condition in the International Bureau's grant of the *pro forma* transfer of control.

49. The record evidence supports the Executive Branch agencies' contention that China Telecom Americas violated certain provisions of the 2007 LOA. The two provisions of the 2007 LOA at issue provide that China Telecom Americas: (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];"¹⁸⁹ and (2) "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."¹⁹⁰ Under the terms of the 2007 LOA, "in the event the commitments set forth in [the 2007 LOA] 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 [China Telecom (USA) Corporation] or any successor-in-interest to . . . [China Telecom (USA) Corporation]."¹⁹¹ Additionally, China Telecom Americas "may have an opportunity to either explain or rectify any such breach."¹⁹²

50. *Take All Practicable Measures to Prevent Unauthorized Access to U.S. Records.* From the record evidence, it appears that China Telecom Americas has not taken all practicable measures to prevent unauthorized access to U.S. records in accordance with its commitments in the 2007 LOA.¹⁹³

51. In particular, China Telecom Americas {{

¹⁸⁸ See *P & R Temmer v. FCC*, 743 F.2d 918 (D.C. Cir. 1984); *Atlantic Richfield Co. v. United States*, 774 F.2d 1193 (D.C. Cir. 1985); see also *Morris Communications, Inc. v. FCC*, 566 F.3d 184 (D.C. Cir. 2009) (automatic termination for non-payment did not violate administrative due process because in such situation "the licenses themselves . . . lapsed"); *Alpine PCS, Inc. et al.; Requests for Waiver of the Installment Payment Rules and Reinstatement of Licenses*, Memorandum Opinion and Order, 25 FCC Rcd 469 (2010), *aff'd*, 404 Fed. Appx. 508 (D.C. Cir. 2010) (provision for automatic cancellation did not trigger section 312(a) revocation procedures).

¹⁸⁹ Executive Branch Recommendation to Revoke and Terminate at 53; 2007 LOA at 2.

¹⁹⁰ Executive Branch Recommendation to Revoke and Terminate at 53; 2007 LOA at 2-3.

¹⁹¹ Executive Branch Recommendation to Revoke and Terminate at 53-54; 2007 LOA at 3.

¹⁹² 2007 LOA at 3.

¹⁹³ Executive Branch Recommendation to Revoke and Terminate at 53-55; 2007 LOA at 2.

¹⁹⁴ Executive Branch Recommendation to Revoke and Terminate at 54. {{

}} *Id.* (citing *id.*, Business Confidential Exh. 119 at EB-2745; *id.*, Business Confidential Exh. 124 at EB-2775-76).

¹⁹⁵ {{

}}¹⁹⁶ The record evidence also shows that when “Team Telecom asked for copies of [China Telecom Americas’] cybersecurity policies in order to monitor compliance with the LOA’s requirement that [China Telecom Americas] ‘take all practicable measures’ to prevent unauthorized access to U.S. Records,” China Telecom Americas “did not immediately disclose that {{

}}¹⁹⁷ The Executive Branch agencies argue that {{

}}¹⁹⁸

52. China Telecom Americas argues that the 2007 LOA “does not require [China Telecom Americas] to implement a single, comprehensive cybersecurity policy . . . [or] have any ‘written’ information security document(s) or policy(ies) at all.”¹⁹⁹ In its response, China Telecom Americas states that “[a]lthough the Information Security Policy provided in December 2018 was the ‘first formal, comprehensive security policy,’ it was not [China Telecom Americas’] first (or only) policy governing its security practices.”²⁰⁰ China Telecom Americas adds that the Information Security Policy was an effort to “memorialize numerous cybersecurity and privacy policies already implemented by [China Telecom Americas].”²⁰¹ Though the 2007 LOA may not specify the exact measures for a cybersecurity policy (or

(Continued from previous page) _____

}} *Id.*, Business Confidential Exh. 124 at EB-2777 (emphasis added). {{

}} *See id.*, Business Confidential Exh. 36 at EB-589-619; *id.*, Business Confidential Exh. 32 at EB-576.

¹⁹⁶ *Id.* at 54 (comparing *id.*, Business Confidential Exh. 103 at EB-2113 {{
}} with *id.*, Business Confidential Exh. 36 at EB-624 {{

}}).

¹⁹⁷ *Id.* at 17.

¹⁹⁸ *Id.* at 54 (citing *id.*, Business Confidential Exh. 102 at EB-2103; *id.*, Business Confidential Exh. 109 at EB-2170, Letter from Morgan Lewis to DOJ National Security Division (Mar. 27, 2019); *id.*, Business Confidential Exh. 103 at EB-2107; *id.*, Business Confidential Exh. 119 at EB-2745; *id.*, Business Confidential Exh. 124 at EB-2774).

¹⁹⁹ China Telecom Americas Response, Exh. 16 at 65-66. China Telecom Americas also contends that “[China Telecom Americas’] LOA [does not] specify the provisions or issues that should be included, impose cybersecurity standards [China Telecom Americas] must follow, or set a timeline for when such any specific policy or standard must be implemented.” *Id.* at 66. China Telecom Americas argues that “the fact that [China Telecom Americas] fulfilled its obligations in a different manner than Team Telecom might have preferred cannot constitute a breach of the LOA.” *Id.* China Telecom Americas contends that “[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 [China Telecom Americas] failed to take measures to protect its customer information, or that it breached its obligations under the LOA.” *Id.* at 69.

²⁰⁰ *Id.* at 66 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 37 at EB-655).

²⁰¹ *Id.* at 39.

that it must be in writing), we have no evidence of what measures (if any) China Telecom Americas adopted to comply with the requirements of the 2007 LOA. China Telecom Americas states that it “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 [China Telecom Americas] actually collects and maintains in the course of provisioning and billing services to customers,” but it does not explain the measures in detail, provide copies of the policies to the Commission or any evidence to prove when the policies were effective, or state how these measures protect the U.S. records.²⁰² China Telecom Americas states that it “also has Physical Access Guidelines and Policies (‘Physical Access Policies’) that outline strict controls for access to [China Telecom Americas’] POPs and data centers,” follows industry standards,²⁰³ and references {{

}}²⁰⁴ However, China Telecom Americas does not 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 {{ }}²⁰⁵ Based on these facts, these measures simply do not rise to the level of “practicable measures” that would prevent unauthorized access to U.S. records, and in any event fail to explain China Telecom Americas’ apparent lack of compliance with the 2007 LOA for over ten years.²⁰⁶ Based on the record evidence, China Telecom Americas’ arguments are unpersuasive.

53. China Telecom Americas’ rebuttals to the substantial concerns raised by the Executive Branch agencies, and its apparent lack of transparency in its interactions with these agencies, suggest that China Telecom Americas failed to take “all practicable measures” required under the 2007 LOA to

²⁰² *Id.* at 66; *see also* Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2108 ({{

}}).

²⁰³ China Telecom Americas Response, Exh. 16 at 67-68.

²⁰⁴ *Id.* at 67 (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 103 at EB-2113).

²⁰⁵ {{

}} Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 36 at EB-589-91, EB-642-654; *see also* China Telecom Americas Response, Exh. 16 at 40-41 (“[T]eam Telecom sent a further request seeking an explanation of [China Telecom Americas’] CALEA compliance policy and a ‘list [of] other companies that are used by [China Telecom Americas] and CTExcel to fulfil (sic) all government legal service.’ Following these numerous requests and correspondence between Team Telecom and counsel for [China Telecom Americas], [China Telecom Americas] submitted its Information Security Policy and responses to Team Telecom’s additional questions on December 6, 2018.”) (citing Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 35 at EB-585; *id.*, Business Confidential Exh. 36, EB-589-654).

²⁰⁶ *See* Executive Branch Recommendation to Revoke and Terminate at 54.

prevent unauthorized access to U.S. records.²⁰⁷ Our view is supported by China Telecom Americas’
 {{

}}²¹⁰ As NTIA explained, “this information is necessary for the Executive Branch’s assessment of whether an application raises national security or law enforcement concerns”²¹¹ and assists the Executive Branch agencies to “determine whether it needs to negotiate a mitigation agreement.”²¹²

54. We therefore give weight to China Telecom Americas’ {{

}} It is also understandable why the Executive Branch agencies would be concerned when {{

²⁰⁷ *Id.* at 53; 2007 LOA at 2 (Under the 2007 LOA, China Telecom Americas has committed 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 the commitments set forth [in the 2007 LOA].”).

²⁰⁸ Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15.

²⁰⁹ *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10929, para. 5.

²¹⁰ Executive Branch Recommendation to Revoke and Terminate at 21; *id.*, Business Confidential Exh. 3 at EB-15.

²¹¹ *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10943, para. 42; *see also id.* at 10929, para. 5 & n.5.

²¹² *Id.*, 35 FCC Rcd at 10929, para. 5. We recently issued the *Executive Branch Process Reform 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. *Id.* 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.”).

²¹³ Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 3 at EB-15.

²¹⁴ *Id.* at 19 (citing *id.*, Business Confidential Exh. 36 at EB-624). {{

(continued....)

}} “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].”²¹⁶ {{

}} These concerns are particularly heightened in light of the national security and law enforcement concerns that the Executive Branch agencies have identified regarding access to China Telecom Americas’ U.S. records by non-U.S. affiliated entities.

55. *Notify Executive Branch Agencies of Applications for ISPCs.* From the record evidence, it appears that China Telecom Americas has breached the 2007 LOA provision requiring that China Telecom Americas “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.”²¹⁹ Specifically, the Executive Branch agencies contend that “[China Telecom Americas] failed to inform the FBI, DOJ and DHS at least twice in 2010 when it filed notices to the FCC,”²²⁰ citing applications for ISPCs in File Nos. SPC-NEW-20100314-00006 and SPC-NEW-20100326-00007.²²¹ The

(Continued from previous page) _____

}} *Id.*, Business Confidential Exh. 36 at EB-624 (emphasis added). {

}} *Id.* (emphasis added).

²¹⁵ *Id.* at 21; *see also* Petition to Adopt Conditions to Authorizations and Licenses.

²¹⁶ 2007 LOA at 2.

²¹⁷ Executive Branch Recommendation to Revoke and Terminate at 19 (citing *id.*, Business Confidential Exh. 103 at EB-2111-12, Letter from Morgan Lewis to DOJ National Security Division (April 4, 2019)).

²¹⁸ China Telecom Americas Response, Exh. 16 at 21.

²¹⁹ 2007 LOA at 2-3.

²²⁰ Executive Branch Recommendation to Revoke and Terminate at 55 & n.199 (citing *id.*, Business Confidential Exh. 103 at EB-2108-09 and File Nos. SPC-NEW-20100326-00007 and SPC-NEW-20100314-00006).

²²¹ *Id.* at 55 & n.199 (citing *id.*, Business Confidential Exh. 103 at EB-2108-2109 and File Nos. SPC-NEW-20100326-00007 and SPC-NEW-20100314-00006); *see also id.*, Business Confidential Exh. 102 at EB-2103 ({{

(continued....)

Executive Branch agencies assert that {{

}}²²²

56. A plain reading of the 2007 LOA supports the Executive Branch agencies' contention that China Telecom Americas breached this provision of the 2007 LOA. By its terms, the 2007 LOA requires that China Telecom Americas "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."²²³ In this case, the record evidence shows that China Telecom Americas filed applications for ISPCs with the Commission without prior notification to the Executive Branch agencies.²²⁴ 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 China Telecom Americas' dealings with the Commission, which did not happen here.

57. China Telecom Americas does not dispute that it did not notify the Executive Branch agencies of its applications for the ISPCs. Rather, China Telecom Americas characterizes such applications as "trivial, ministerial filings" that do not require prior notification to the Executive Branch agencies.²²⁵ As support, China Telecom Americas contends that the 2007 LOA provision "must be

(Continued from previous page) _____

}); *id.*, Business Confidential Exh. 119 at EB-2746

{{

}}).

²²² *Id.* at 55 (citing *id.*, Business Confidential Exh. 103 at EB-2108; *id.*, Business Confidential Exh. 119 at EB-2745-46; *id.*, Business Confidential Exh. 124 at EB-2774); *see also id.*, Business Confidential Exh. 102 at EB-2103

{{

}}).

²²³ 2007 LOA at 2-3 (emphasis added).

²²⁴ Executive Branch Recommendation to Revoke and Terminate at 55. The record evidence also shows that {{

}} *See id.*, Business Confidential

Exh. 119 at EB-2746, May 29, 2019 Letter from DOJ National Security Division to Morgan Lewis ({{

}}); *id.*, Business Confidential Exh. 103 at EB-2108-09, Apr. 4, 2019 Letter from Morgan Lewis to DOJ National Security Division ({{

}}).

²²⁵ China Telecom Americas Response, Exh. 16 at 69-70. China Telecom Americas states that "[t]hese requests were submitted using the 'application' interface of the International Bureau Filing System ('IBFS'). This 'application,' however, is purely ministerial. The application form only requires the identity of the carrier and certification that the carrier understands and accepts the terms on which the code is assigned. The Commission performs no substantive review of this information." *Id.* at 69.

interpreted in its entirety and not by taking portions out of context,” postulating that “[i]f the LOA only required [China Telecom Americas] 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.”²²⁶ China Telecom Americas states that “[t]he request for assignment of additional ISPCs was not a material change in [China Telecom Americas’] business or services.”²²⁷ In the alternative, China Telecom Americas argues 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.”²²⁸

58. While China Telecom Americas may view an application for an ISPC as “purely ministerial,”²²⁹ in fact, 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.²³⁰ Relatedly, the International Bureau recently reclaimed China Telecom Americas’ three ISPCs as “China Telecom Americas is not in compliance with the conditions of its provisional ISPC assignments.”²³¹ Reclamation of China Telecom Americas’ ISPCs was due to China Telecom Americas’ 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. Despite China Telecom Americas’ claims, the assignment of international SS7 routing addresses remains a non-trivial resource regardless of whether, or to what extent, China Telecom Americas chooses to deploy SS7.

59. Moreover, we are not persuaded by China Telecom Americas’ 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.”²³² As stated by the Executive Branch agencies, “[d]espite regular compliance monitoring, the U.S. government can never have full visibility into all of a company’s activities and must rely on the private party to adhere rigorously and scrupulously to mitigation agreements and to self-report instances of non-compliance.”²³³ 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 China Telecom Americas’ 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 China Telecom Americas responded to the Executive Branch agencies’ inquiries on this matter. For

²²⁶ *Id.* at 70.

²²⁷ *Id.* (stating that “[China Telecom Americas] first obtained an ISPC in 2003, long before it signed the LOA (a fact known to the FCC and Team Telecom when [China Telecom Americas] entered into the LOA).”).

²²⁸ *Id.*

²²⁹ *Id.* at 69.

²³⁰ International Telecommunication Union, ITU-T Recommendation Q.708 (03/99), Series Q: Switching and Signalling, Specifications of Signalling System No. 7 – Message Transfer Part (MTP), Assignment procedures for international signalling point codes, <https://www.itu.int/rec/recommendation.asp?lang=en&parent=T-REC-Q.708-199903-I>. The Commission has adopted rules requiring applicants to submit ISPC applications electronically via the International Bureau Filing System (IBFS) and stating that the Commission will take action on ISPC applications via a letter issued to the applicant. See 47 CFR §§ 1.10007(a), 1.10014(h).

²³¹ See ISPC Reclamation Letter at 1.

²³² China Telecom Americas Response, Exh. 16 at 70.

²³³ Executive Branch Recommendation to Revoke and Terminate at 55.

these reasons, China Telecom Americas' failure to notify the Executive Branch agencies of its applications for the ISPCs appears to constitute a breach of the conditions of the grant of the *pro forma* transfer of control, which requires compliance with the terms of the 2007 LOA.

60. *Executive Branch Agencies Do Not Recommend Further Mitigation.* The Executive Branch agencies assert that they do not recommend further mitigation, "because 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."²³⁴ The Executive Branch agencies contend that "[China Telecom Americas'] failure to comply with two of the five provisions in a modest, three-page LOA, or to propose additional mitigation when confronted with these breaches, demonstrates that [China Telecom Americas] should not be trusted to comply with more stringent mitigation measures."²³⁵ The Executive Branch agencies assert that "[e]ven if [China Telecom Americas] had proposed mitigation measures, they would likely be insufficient to address newly discovered risks in today's rapidly evolving threat environment."²³⁶ In response, China Telecom Americas asserts, for example, that "Team Telecom dictates mitigation measures to companies, essentially on a take-it-or-leave-it basis."²³⁷ China Telecom Americas argues that "the Administrative Procedure Act seems to require that the Commission give [China Telecom Americas] an opportunity to mitigate any risks that it might identify."²³⁸

61. We are unpersuaded by China Telecom Americas' arguments. The proceeding that we institute today will afford China Telecom Americas an additional opportunity to present arguments and evidence regarding whether the Commission should revoke its domestic section 214 authority and revoke and/or terminate its international section 214 authorizations. Moreover, China Telecom Americas had various opportunities to propose additional mitigation measures when it was originally alerted of its LOA breaches, but failed to do so. The record evidence shows that {[

]}²³⁹ We find that the record reflecting China Telecom Americas' 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 China Telecom Americas' vulnerability to the exploitation, influence, and control of the Chinese government, raise serious concerns as to whether China Telecom Americas 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. We disagree with China Telecom Americas' suggestion that the APA

²³⁴ *Id.* at 53.

²³⁵ *Id.* at 55.

²³⁶ *Id.*

²³⁷ China Telecom Americas Response, Exh. 16 at 71.

²³⁸ *Id.*

²³⁹ Executive Branch Recommendation to Revoke and Terminate, Business Confidential Exh. 102 at EB-2103, Mar. 21, 2019 Letter from DOJ National Security Division to Morgan Lewis ({{

}}); *id.*, Business Confidential Exh. 119 at EB-2745-46, May 29, 2019 Letter from DOJ National Security Division to Morgan Lewis ({{

}}).

requires more process than we are providing here.²⁴⁰ Section 558(c)(2) does not grant a substantive right to escape from a condition that terminates a license.²⁴¹

IV. MEMORANDUM OPINION AND ORDER

62. China Telecom Americas seeks review of the International Bureau's determination that pursuant to section 0.442 of our regulations, the Committee should be provided the versions of Exhibit 16 of its Response to the Order to Show Cause and the various exhibits cited in Exhibit 16 that were submitted to the Commission as confidential.²⁴² In this Memorandum Opinion and Order, we affirm.²⁴³

63. As a threshold matter, China Telecom Americas argues that the criteria for establishing a legitimate need for information under section 0.442 is a new or novel question that cannot be answered by the International Bureau on delegated authority.²⁴⁴ Because the International Bureau's decision was *ultra vires*, China Telecom Americas argues, the Commission should vacate and reverse the decision. We disagree with both China Telecom Americas' argument and its proposed remedy.

64. To begin with, the International Bureau's determination did not decide any novel issues of law or policy: The Commission's various bureaus and offices frequently disclose confidential information to other federal agencies pursuant to section 0.442 and the terms of the regulation are not particularly unclear. Even if China Telecom Americas were correct, however, we disagree that this argument would compel us to vacate and reverse the International Bureau's determination. In the end, we believe the International Bureau was correct in ordering the release of this information, and our Commission-level decision on this issue renders moot any question about the scope of the International Bureau's authority.

65. We turn next to China Telecom Americas' substantive argument, which we likewise find unpersuasive. The disclosure to other federal government agencies of information submitted to the Commission in confidence is generally governed by 44 U.S.C. section 3510 and our implementing regulation, 47 CFR section 0.442.²⁴⁵ Such information may be disclosed to another federal agency at its request or on our own motion, provided that four conditions are met.²⁴⁶ We find that each of these four conditions have been met here. The Commission has not given China Telecom Americas specific assurances that its information would not be to disclosed other federal government agencies; disclosing

²⁴⁰ China Telecom Americas Response, Exh. 16 at 71.

²⁴¹ 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") (internal quotation and citations omitted).

²⁴² Application for Review; Disclosure Ruling.

Information submitted to the Commission in confidence is maintained as confidential until the Commission rules on the request or otherwise decides to publicly disclose the information. See 47 CFR §§ 0.457, 0.459(d)(3), 0.461(f)(4). We need not decide here whether and to what extent the assertions of confidentiality made by China Telecom Americas are consistent with Commission rules, regulations, and policies in this regard.

²⁴³ Our rules provide that we may disclose confidential information to other federal agencies upon their request or upon our own motion. 47 CFR § 0.442(b).

²⁴⁴ Application for Review at 2-4.

²⁴⁵ 44 U.S.C. § 3510; 47 CFR § 0.442.

²⁴⁶ 47 CFR § 0.442(b). These conditions are the following: "(1) [s]pecific Commission assurances against such disclosure have not been given; (2) [t]he other agency has established a legitimate need for the information; (3) [d]isclosure is made subject to the provisions of 44 U.S.C. 3510(b); and (4) [d]isclosure is not prohibited by the Privacy Act or other provisions of law." *Id.*

the information is not otherwise prohibited by law; the disclosure is being made subject to the provisions of the statute, which require that the Committee maintain the confidentiality of the information; and the Committee has a legitimate need for the information. China Telecom Americas takes issue with these last two conditions.

66. *First*, China Telecom Americas argues that the Commission has not ensured that the Committee will keep the information confidential, as required by section 3510(b) and the Commission's rules.²⁴⁷ We disagree. DOJ, on behalf of the Committee, has assured in writing that the agencies will protect the confidentiality of the requested information as specified by the Commission's regulations as well as by their own agency's regulations, as section 3510(b) requires. What is more, the International Bureau's disclosure of the information to the Committee was explicitly made subject to the requirements of section 3510(b).²⁴⁸ Through the statute and our regulations, China Telecom Americas receives the confidentiality protections not only of the Commission's regulations but also of the various agencies that receive its information. We also note that all federal employees are also bound by the Trade Secrets Act, 18 U.S.C. § 1905, which provides criminal and employment penalties for the unauthorized disclosure of confidential business information.²⁴⁹ China Telecom Americas' argument that the disclosure of the information to the Committee is wholly devoid of any conditions for continuing responsibility for safeguarding the information from disclosure or consequences for disclosure²⁵⁰ is therefore incorrect, as is its argument that there is no assurance that the confidentiality and limitation of use of the information will be respected.²⁵¹ And while China Telecom Americas may be correct that additional people will have access to its confidential information,²⁵² there is simply no reason to believe that these federal agencies and their employees will not properly guard and maintain the confidentiality of that information as they are required to do by regulation and statute. In short, we find that the confidentiality protections required by that section (described above) more than adequately protect China Telecom Americas' confidential information and we reject China Telecom Americas' arguments that the protections are somehow inadequate or insufficient. At bottom, the disclosures are made subject to section 3510(b). Satisfying this element of the Commission's rules requires nothing more.

67. *Second*, China Telecom Americas argues that the Committee has not established a "legitimate need" for the information.²⁵³ Much of its argument revolves around the fact that the *Order to Show Cause* did not require the Committee to file a response to China Telecom Americas' reply and therefore that the Committee had no need for any further information—that in making its initial recommendation to the Commission, it had done all it was required to do.²⁵⁴ We agree with the International Bureau that the Order did not prohibit the Committee from filing a response and that it could have filed one if it thought it useful.²⁵⁵ It could not fully make that determination, of course, without

²⁴⁷ Application for Review at 7-9; *see also* 47 CFR § 0.442(b)(3) (requiring that "[d]isclosure is made subject to the provisions of 44 U.S.C. 3510(b)").

²⁴⁸ Disclosure Ruling, 35 FCC Rcd at 8776.

²⁴⁹ 18 U.S.C. § 1905.

²⁵⁰ Application for Review at 8; *see also id.* at 4-5.

²⁵¹ *Id.* at 5.

²⁵² *Id.* at 4-5, 7-8.

²⁵³ *See also* 47 CFR § 0.442(b)(2) (requiring that "[t]he other agency has established a legitimate need for the information").

²⁵⁴ Application for Review at 4-6.

²⁵⁵ Disclosure Ruling, 35 FCC Rcd at 8777.

reviewing the confidential information at issue. We therefore agree with the International Bureau's decision.

68. But in any event, our decision to initiate further proceedings in this matter renders moot this argument by establishing an even clearer need for the Executive Branch to have access to this information. Today, we provide an opportunity for the public, including other government agencies, to respond to China Telecom Americas' most recent filing. Although DOJ and the Committee are not required to participate in this proceeding, given that the Committee's request stated it needed the information "to evaluate China Telecom Americas' response to the Executive Branch's recommendation and respond fully to the arguments raised by China Telecom Americas,"²⁵⁶ we fully expect it to do so, and in any event, it will need to review the information that was submitted by China Telecom Americas to determine whether there are any arguments that might require a response. We therefore find that this is a legitimate need for the information, a point with which China Telecom Americas at least implicitly agrees.²⁵⁷ More generally, we have recently held that the Committee's role in ensuring the "[t]he security, integrity, and availability of the United States telecommunications networks [that] are vital to United States national security and law enforcement interests,"²⁵⁸ means that the Committee has a legitimate need to see confidential business information filed by applicants or authorization holders when the Commission is reviewing its recommendations, and that we will provide the Committee with that information.²⁵⁹

69. China Telecom Americas also argues that even if the Commission generally needs its confidential information, the Committee does not need to know the names of its customers and the services it provides them.²⁶⁰ We note, as did the International Bureau, that the Committee is charged by law with assisting the Commission "in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector" and with responding "to any risks presented by . . . licenses by recommending to the FCC, as appropriate and consistent with the provisions of this order, that it . . . modify a license with a condition of compliance with mitigation measures, or revoke a license."²⁶¹ To determine the concerns and risks involved in China Telecom Americas continuing to hold FCC authorizations, one must determine the *extent* of those risks, and we find that knowing the identity of China Telecom Americas' customers and the service it provides them is extremely relevant to that determination. More generally, for the Committee to assist us in our public interest review, it must have access to all of the information that we have that relates to potential national security and law enforcement concerns. It is, in fact, difficult to conceive of any confidential information that the Commission would consider relevant to its determination as to whether China Telecom Americas' authorizations should be revoked that would not

²⁵⁶ Department of Justice July 8, 2020 Letter.

²⁵⁷ See Application for Review at 5 (China Telecom Americas fully expects any revocation proceeding to include the opportunity for participants to seek access to confidential information).

²⁵⁸ Executive Order 13913, 85 Fed. Reg. at 19643 § 1.

²⁵⁹ *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10964-65, 10979, para. 93, new rule section 1.40001(b), (c) (rules to become effective Dec. 28, 2020). No commenter opposed the Commission's sharing confidential information with the Committee. *Id.* at 10964, para. 93.

²⁶⁰ Application for Review at 6-8. While China Telecom Americas raises confidentiality concerns on its customers' behalf as well as its own, we note that none of those customers have come to the Commission to object about the release of this information to the Committee.

²⁶¹ See Executive Order 13913, 85 Fed. Reg. at 19643-44 § 3.

also be relevant for the Committee to review in assisting the Commission in making that determination.²⁶² We therefore reject China Telecom Americas' argument that the Committee has no legitimate need for the identity of its customers and the services it provides them, as well as its argument that because it is required by its 2007 LOA to provide all relevant information to the Committee, the Committee does not need information submitted to the Commission.²⁶³

70. The Application for Review of China Telecom Americas is therefore denied. China Telecom Americas will have ten (10) calendar days from the date of the release of this Order to move for a judicial stay of the disclosure. If it does not move for a stay within that time, then the information will be disclosed consistent with the terms of this Order.²⁶⁴

V. PROCEDURAL MATTERS

71. *Written Submissions.* The public, including the Committee, may file comments responding to the Response of China Telecom (Americas) Corporation to Order to Show Cause, filed with the Commission on June 8, 2020. Such comments may be filed no later than January 19, 2021. Any filing by China Telecom Americas demonstrating why the Commission should not revoke and/or terminate its section 214 authority may be submitted no later than March 1, 2021. All filings concerning matters referenced in this Order should refer to GN Docket No. 20-109.

72. *Ex Parte Presentations.* The proceeding this Order initiates shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.²⁶⁵ Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native

²⁶² Indeed, in adopting our new rules regarding the Committee's review of applications and authorizations, we did not limit the types of confidential business information we would provide the Committee. See *Executive Branch Process Reform Report and Order*, 35 FCC Rcd at 10964-65, para. 93.

²⁶³ Application for Review at 7. In fact, China Telecom Americas' emphasis that it must provide all "relevant" information to the Committee (*see, e.g., id.* at 5) in response to "legitimate" requests (*id.* at 9) implies that it is making its own determinations as to what is relevant and that it may not be providing the Committee all of the information required by the Letter. We find that the ability for the Committee to verify that it is indeed receiving all of the information it is supposed to be constitutes yet another legitimate need to receive the confidential information China Telecom Americas submits to the Commission.

²⁶⁴ See 47 CFR § 0.442(d)(4).

²⁶⁵ 47 CFR §§ 1.1200 *et seq.*

format (e.g., .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

73. *Filing Procedures.* Filings in this proceeding must be filed in the Commission's Electronic Comment Filing System (ECFS) in GN Docket No. 20-109.

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing.
- Filings can be sent by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9050 Junction Drive, Annapolis Junction, MD 20701. U.S. Postal Service first-class, Express, and Priority mail must be addressed to 45 L Street NE Washington, DC 20554.
- Effective March 19, 2020, and until further notice, the Commission no longer accepts any hand or messenger delivered filings. This is a temporary measure taken to help protect the health and safety of individuals, and to mitigate the transmission of COVID-19. See FCC Announces Closure of FCC Headquarters Open Window and Change in Hand-Delivery Policy, Public Notice, DA 20-304 (March 19, 2020). <https://www.fcc.gov/document/fcc-closes-headquarters-open-window-and-changes-hand-delivery-policy>

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

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

VI. ORDERING CLAUSES

76. Accordingly, IT IS ORDERED that, pursuant to sections 4(i), 4(j), 214, 215, 218, and 403 of the Act, section 1.1 of the Commission's rules,²⁶⁶ the public MAY FILE a written response to the Response of China Telecom (Americas) Corporation to Order to Show Cause, filed with the Commission on June 8, 2020, no later than **January 19, 2021**. Any filing by China Telecom (Americas) Corporation demonstrating why the Commission should not revoke and/or terminate its section 214 authority may be submitted no later than **March 1, 2021**.

77. IT IS FURTHER ORDERED that the Application for Review of China Telecom (Americas) Corporation filed on August 31, 2020, is DENIED.

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

China Telecom (Americas) Corporation
c/o Andrew D. Lipman
Catherine Wang
Russell M. Blau
Raechel Keay Kummer

²⁶⁶ 47 U.S.C. §§ 154(i), 154(j), 214, 215, 218, 403.

Frank G. Lamancusa
Morgan, Lewis and Bockius LLP
1111 Pennsylvania Ave., NW
Washington, D.C. 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
D.C. Agent for Service of Process
The Compliance Group, Inc.
1300 I Street, NW, Suite 400E
Washington, D.C. 20005

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

**STATEMENT OF
CHAIRMAN AJIT PAI**

Re: *China Telecom (Americas) Corporation*, GN Docket No. 20-109, ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285

Today, we initiate a proceeding to end China Telecom (Americas) Corporation's authority to provide domestic interstate and international telecommunications services within the United States. And for good reason.

Earlier this year, several Executive Branch agencies recommended that we revoke and terminate China Telecom Americas' international section 214 authorizations. Among other troubling allegations, the Executive Branch agencies maintain that China Telecom Americas has failed to comply not only with prior commitments it made in order to retain access to the U.S. market but also with federal and state cybersecurity and privacy laws. The Executive Branch agencies further contend that China Telecom Americas' operations "provide opportunities for increased Chinese state-sponsored cyber activities, including economic espionage and the disruption and misrouting of U.S. communications traffic."

China Telecom Americas is ultimately owned and controlled by the government of the People's Republic of China, which is of course dominated by the Chinese Communist Party. And in January 2018, China Telecom Americas' parent company amended its Articles of Association to give the Chinese Communist Party greater control over its management and operations. These changes, combined with recently enacted Chinese laws, "raise significant concerns that [China Telecom Americas] will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests," according to the Executive Branch agencies.

Moreover, China Telecom Americas' international section 214 authority is conditioned upon it abiding by the commitments it made in a 2007 letter of assurances to the Department of Justice, the Federal Bureau of Investigation, and the Department of Homeland Security. But there are troubling indications that China Telecom Americas has not done so. For example, China Telecom Americas purportedly made inaccurate statements to U.S. authorities about where it stored U.S. records. And it failed to notify Executive Branch agencies when it filed applications with the FCC for International Signaling Point Code assignments—a requirement of its mitigation agreement with the Executive Branch. China Telecom Americas has also allegedly failed to respond promptly to requests for information made by the federal government.

Taken together, these allegations raise serious doubts about whether China Telecom Americas 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. We are therefore compelled to act to protect the integrity of our telecommunications networks and our national security. Specifically, we institute proceedings to revoke and terminate China Telecom Americas' authority to operate in the United States while ensuring that the company is afforded a full and fair opportunity to explain itself. This decision, along with many others we have made since 2017, demonstrates that this FCC is determined to protect the security of America's communications networks.

I want to thank the FCC staff who have worked on this important item: From the International Bureau: Denise Coca, Kate Collins, Francis Gutierrez, Jocelyn Jeziorny, Gabrielle Kim, Tom Sullivan, and Troy Tanner; from the Wireline Competition Bureau: Pamela Arluk, Dennis Johnson, Jodie May, Kris Monteith, Ramesh Nagarajan, and Terri Natoli; from the Enforcement Bureau: Michael Engel, Jeffrey Gee, Rosemary Harold, and Pamela Kane; from the Office of Economics and Analytics: Robert Cannon, Wayne Leighton, Giulia McHenry, Virginia Metallo, and Emily Talaga; from the Public Safety and Homeland Security Bureau: Kenneth Carlberg, Jeffery Goldthorp, and Debra Jordan; and from the Office of General Counsel: Michael Carlson, Tom Johnson, Doug Klein, David Konczal, Joel Rabinovitz, Bill Richardson, and Royce Sherlock.

**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

Last year, 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, and we have sought answers from them to assess any threats they pose to America's national security.

To assist the FCC in our review, the Executive Branch agencies with responsibility for national security reviews have offered their recommendations. They advise that there are now substantial and unacceptable national security and law enforcement risks associated with China Telecom Americas' continued access to U.S. telecommunications infrastructure. They state 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. And our own review reveals that China Telecom Americas' operations appear to provide opportunities for Chinese state-sponsored actors to disrupt and misroute U.S. communications traffic.

When you combine this and other evidence with the particular place in the U.S. communications network where China Telecom Americas operates, the concerns we have raised are only heightened. I therefore agree with the Commission's determination today.

I want to thank the staff of the International Bureau, Wireline Competition Bureau, and Enforcement Bureau for their hard work on this important item. It 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

Network security is national security, and as the communications landscape evolves with new technologies and new business models, the Commission must keep up in order to stay vigilant to threats to our networks. Today, we address one such threat – the presence of adversary state-owned or controlled carriers in American networks.

This item begins the process of revoking the authority of the US affiliate of China’s largest carrier, China Telecom, to operate in the United States. Last year, this Commission rejected an application from the US affiliate of China Mobile, the largest mobile provider in the world, to operate in the United States. We found that China Mobile USA was ultimately owned and controlled by the Chinese government and therefore vulnerable to its exploitation and control, posing a significant risk to both our national security and law enforcement interests.

China Telecom Americas is even more closely aligned with the Chinese government and presents an even graver security risk. The company’s Chinese parent company is majority-owned and controlled by a Chinese government-owned enterprise. Further, the parent company is directly accountable to the Chinese Communist Party and must consult its representatives prior to making any decisions on material issues. In addition, like China Mobile USA, China Telecom Americas is subject to the Chinese government’s legal requirement that all Chinese companies must disclose sensitive customer information upon demand.

The issues aren’t just structural – they’re behavioral. National security agencies say that China Telecom Americas has misrouted large amounts of communications from the United States for many years, including at least 10 incidents, sometimes involving US government traffic. Moreover, when the company sought authority to operate in the United States, it made certain commitments to our national security agencies. I believe the evidence demonstrating that China Telecom Americas, however, has repeatedly violated those commitments. For example, China Telecom Americas has failed to respond in an accurate and timely manner to Team Telecom requests for information and made inaccurate statements about its cybersecurity practices and its handling of U.S. customer records. According to the national security agencies, there are no mitigation measures that would make them comfortable with China Telecom Americas’ continued operation in the United States. I agree and look forward to reviewing proposed actions regarding similarly situated carriers in the future.

But the Commission has other national security issues before it. These issues are handled by many other parts of the agency. For example, earlier today, we approved an order from the Wireline Competition Bureau in our supply chain proceeding to address the problem of equipment from untrustworthy vendors in our wireless networks. I’ve discussed my thoughts on that action separately.

Adversary states are also trying to exploit our broadcast communications. Over the past two years, news outlets have reported on Russian propaganda airing on radio stations in California, my hometown of Kansas City, and even here in Washington, D.C. Earlier this year, the Commission adopted an order from the Media Bureau proposing disclosure requirements for foreign government-provided programming on American stations. We need to finalize those requirements quickly.

Finally, US communications traffic doesn’t stop at the border. Undersea cables carry 99% of the world’s data traffic. The FCC’s International Bureau acts on applications for licenses to own and operate submarine cables and associated landing stations in the United States. As I’ve stated before, we need to focus on who owns, builds, and operates these cables or we risk permitting adversary states and criminals to tamper with, block, or illegally access our communications networks. In particular, China has focused on controlling, building, and owning these cables. Indeed, some of the cables connecting the United

States and China right now are owned in part by China Telecom, the ultimate parent of the very company that is the subject of this proceeding.

These are only a few of the national security proceedings before the FCC, each of which is handled by a different part of the agency. The different parts of the FCC must coordinate their work on those issues so we have strong and consistent policies across the board. Given their importance, I've called for creating an inter-bureau National Security Task Force that would establish a uniform process for reviewing national security issues. Without it, we risk inconsistent treatment of these issues between different bureaus.

I also believe that the FCC should work with the national security and law enforcement agencies to detail staff between our agencies. The Commission's growing national security role requires us to increase our in-house expertise so we can act with confidence in proceedings like this one and work more effectively with our sister agencies. Our world is becoming ever more interconnected – we must ensure that the whole of the FCC is more coordinated, skillful, and collaborative on these critical issues.

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