

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
<b>CHINA TELECOM (AMERICAS) CORPORATION</b>	)	File Nos.
	)	
<b>f/k/a CHINA TELECOM (USA) CORPORATION</b>	)	ITC-214-20010613-00346;
	)	ITC-214-20020716-00371;
	)	ITC-T/C-20070725-00285.
	)	

---

**Executive Branch Recommendation to the Federal Communications Commission to  
Revoke and Terminate China Telecom's International Section 214 Common Carrier  
Authorizations**

**TABLE OF CONTENTS**

I. Introduction .....	1
II. The national security environment has changed significantly since 2007 .....	2
III. China Telecom provides a full suite of communications services in the United States with its international Section 214 authorizations.....	7
IV. The Executive Branch recommends revocation and termination of China Telecom’s international Section 214 authorizations.....	12
A. China Telecom has engaged in conduct that calls its trustworthiness into question (Factor 2).....	17
1. China Telecom made inaccurate statements to Team Telecom about where it stored U.S. records.....	19
2. China Telecom made inaccurate statements to U.S. customers about its cybersecurity practices and may have failed to comply with U.S. cybersecurity and privacy laws .....	26
B. China Telecom is owned and controlled by Chinese parent entities and ultimately by the Chinese government (Factors 3 and 4) .....	32
C. Due to its ownership, China Telecom will be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight (Factors 6-7).....	37
D. China Telecom’s U.S. operations provide opportunities for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic (Factors 5, 8-12).....	41
1. China Telecom’s U.S. operations provide opportunities for Chinese government-sponsored actors to engage in economic espionage against U.S. targets (Factors 5, 9-12) .....	41
2. China Telecom’s operations in the United States provide opportunities for Chinese government-sponsored actors to disrupt and misroute U.S. communications traffic (Factors 8-10, 12).....	44
E. China Telecom’s lack of trustworthiness limits the Executive Branch’s ability to conduct statutorily authorized law enforcement and national security missions, and to protect information about targets and classified sources and missions (Factors 13, 14)..	51
V. The Executive Branch does not recommend further mitigation.....	53
VI. Conclusion.....	56

## **I. Introduction**

The Executive Branch<sup>1</sup> recommends that the Federal Communications Commission (FCC or Commission) revoke and terminate its 2007 certification that China Telecom (Americas) Corp. (China Telecom) meets the present or future public convenience and necessity requirement under Section 214 of the Communications Act, as amended, 47 U.S.C. § 214(a). This recommendation reflects the substantial and unacceptable national security and law enforcement risks associated with China Telecom's continued access to U.S. telecommunications infrastructure pursuant to its international Section 214 authorizations. The Executive Branch's recommendation 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's status as a subsidiary of a Chinese state-owned enterprise under the ultimate ownership and control of the Chinese government;
- China Telecom's inaccurate statements 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; and
- China Telecom's 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.

---

<sup>1</sup> For purposes of this recommendation, the Executive Branch includes the Departments of Justice (DOJ), Homeland Security (DHS), Defense (DoD), State, Commerce, and the United States Trade Representative (USTR) (collectively, the Executive Branch or Executive Branch Agencies).

In the current environment, the national security and law enforcement risks associated with China Telecom's international Section 214 authorizations cannot be mitigated.

The bases for the Executive Branch's recommendation are set forth in the arguments below and unclassified exhibits appended hereto. The Executive Branch is also submitting a separate classified appendix with additional information relevant to this recommendation, but submits that the unclassified information alone is sufficient to support its recommendation.

## **II. The national security environment has changed significantly since 2007**

The national security environment has changed significantly since 2007, when the Commission last certified China Telecom's international Section 214 authorizations to provide international common carrier services. In 2007, the U.S. Intelligence Community's top concern was terrorism, with the countries of highest concern being Iraq, Afghanistan, and Pakistan.<sup>2</sup> In 2007, the Office of the Director of National Intelligence (ODNI) did not mention the word "cyber" in its annual briefing to Congress on global threats.<sup>3</sup> By 2019, the world had changed: cyber issues are listed at the top of this year's ODNI worldwide threat assessment, and China is the first country identified by name for its persistent economic espionage and growing threat to core military and critical infrastructure systems.<sup>4</sup>

---

<sup>2</sup> Exhibit 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).

<sup>3</sup> *Id.*

<sup>4</sup> Exhibit 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).

The ODNI'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."<sup>5</sup> In July 2018, ODNI's National Counterintelligence and Security Center (NCSC) similarly warned that "the Chinese government seeks to enhance its collection of U.S. technology by enlisting the support of a broad range of actors spread throughout its [ ] industrial base."<sup>6</sup>

The Executive Branch Agencies have raised similar concerns recently. In 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."<sup>7</sup> According to DoD, the access and skill seen in past Chinese intrusions "are similar to those necessary to conduct cyber operations in an attempt to deter, delay, disrupt, and degrade DoD operations prior to or during a conflict."<sup>8</sup> In 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."<sup>9</sup> In September 2018, the White House

---

<sup>5</sup> *Id.* (emphasis added).

<sup>6</sup> Exhibit 82 at EB-1910, *Foreign Economic Espionage in Cyberspace*, National Counterintelligence and Security Center 5 (July 26, 2018), <https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace>.

<sup>7</sup> Exhibit 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>.

<sup>8</sup> *Id.*

<sup>9</sup> Exhibit 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

estimated that “China engaged in cyber-enabled economic espionage and trillions of dollars of intellectual property theft.”<sup>10</sup>

In 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. . . . They’re using an expanding set of nontraditional methods to do that—both lawful and unlawful—from things like foreign investments and corporate acquisitions, to cyber intrusions and supply chain threats.”<sup>11</sup>

By the end of 2018, DOJ had announced multiple indictments of Chinese state actors targeting the U.S. private sector. Since the Economic Espionage Act was passed in 1996, about 80 percent of DOJ’s economic espionage cases (involving trade secret theft where the defendant knew or intended that his theft would benefit a foreign government, instrumentality, or agent) have involved China, and most trade secret theft cases have had some nexus to China. Recently announced criminal charges include:

- The October 10, 2018 unsealing of an indictment against a Chinese intelligence officer for seeking to steal U.S. trade secrets relating to aircraft engine designs;<sup>12</sup>

---

Infrastructure Security Agency, U.S. Department of Homeland Security).

<sup>10</sup> Exhibit 57 at EB-933, *National Cyber Strategy of the United States of America*, White House 2 (Sept. 2018), <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

<sup>11</sup> 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>.

<sup>12</sup> See Exhibit 66 at EB-1442, Press Release, U.S. Dep’t of Justice, *Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S.*

[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

- The October 30, 2018 unsealing of an indictment of Chinese intelligence officers and hackers and co-opted company insiders working for them for targeting U.S. aerospace technology, including information related to a turbofan engine used in commercial airliners;<sup>13</sup>
- The November 1, 2018 unsealing of an indictment charging a Chinese state-owned company, a Taiwanese company, and three individuals for economic espionage related to theft of U.S. trade secrets relating to dynamic random access memory;<sup>14</sup> and
- The December 20, 2018 unsealing of an indictment of two defendants for working in association with a Chinese intelligence service to hack into managed service providers (MSP) and their clients, here and abroad, for the purpose of stealing, among other data, intellectual property and confidential business and technological information of MSP clients in the banking and finance, telecommunications and

---

Aviation Companies (Oct. 10, 2018), <https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading>; *see also* Exhibit 97 at EB-2004, *United States v. Xu*, No. 18-cr-43, Indictment (S.D. Ohio Apr. 4, 2018).

<sup>13</sup> *See* Exhibit 67 at EB-1444, Press Release, U.S. Dep't of Justice, Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years (Oct. 30, 2018), <https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal>; *see also* Exhibit 98 at EB-2020, *United States v. Zhang*, No. 13-cr-3132, Indictment (S.D. Cal. Oct. 25, 2018).

<sup>14</sup> *See* Exhibit 68 at EB-1446, Press Release, U.S. Dep't of Justice, PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage (Nov. 1, 2018), <https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage>; *see also* Exhibit 99 at EB-2041, *United States v. United Microelectronics Corp.*, No. 18-cr-465, Indictment (N.D. Cal. Sept. 27, 2018).

consumer electronics, medical equipment, packaging, manufacturing, consulting, healthcare, biotechnology, automotive, oil and gas exploration, and mining sectors.<sup>15</sup>

The U.S. Trade Representative, in its March 2018 Section 301 findings, reported that “cyber theft [was] one of China’s preferred methods of collecting commercial information because of its [ ] plausible deniability.”<sup>16</sup> Only months later, 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.<sup>17</sup>

Most recently, in May 2019, the FCC echoed concerns raised by the Executive Branch Agencies about China’s access to U.S. telecommunications networks in its unanimous decision denying China Mobile International (USA) Inc.’s application for an international Section 214 authorization.<sup>18</sup> The FCC found 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

---

<sup>15</sup> See Exhibit 69 at EB-1448, Press Release, U.S. Dep’t of Justice, Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information (Dec. 20, 2018), <https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion>; see also Exhibit 100 at EB-2071, *United States v. Zhu*, No. 18-cr-891, Indictment (S.D.N.Y. Dec. 17, 2018).

<sup>16</sup> Exhibit 60 at EB-1135, Office of the U.S. Trade Representative, *Findings of the Investigation into China’s Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, at 153 (Mar. 22, 2018), <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>.

<sup>17</sup> See Exhibit 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>.

<sup>18</sup> *In the Matter of China Mobile Int’l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd. 3361 (May 10, 2019) (*China Mobile Order*).



conduct activities that would seriously jeopardize the national security and law enforcement interests of the United States.”<sup>19</sup>

**III. China Telecom provides a full suite of communications services in the United States with its international Section 214 authorizations**

China Telecom is an international common carrier authorized to provide “international basic switched, private line, data, television and business services”<sup>20</sup> under 47 U.S.C. § 214 and 47 C.F.R. § 63.18(e)(1)-(2).<sup>21</sup> China Telecom’s stated mission is to “deliver high-quality data and voice solutions and services between the Americas and China to businesses and carriers.”<sup>22</sup> Its international Section 214 authorizations, last certified in 2007, are conditioned on China Telecom’s compliance with a Letter of Assurances (LOA) with DOJ, FBI and DHS.<sup>23</sup>

---

<sup>19</sup> *Id.* at 3366 ¶ 8.

<sup>20</sup> 47 C.F.R. § 63.22(d) (facilities-based international common carrier); 47 C.F.R. § 63.23(c) (resale-based international common carrier).

<sup>21</sup> Exhibit 10 at EB-395, *Int’l Authorizations Granted*, 22 FCC Rcd. 15266 (2007) (granting Petition to Adopt Conditions to Authorizations and Licenses filed by DHS with concurrence of DOJ and FBI, and conditioning grant of authorization of pro forma transfer of control of international Section 214 authorizations); Exhibit 11 at EB-400, *Int’l Authorizations Granted*, 17 FCC Rcd. 16199 (2002) (authorizing China Telecom (USA) Corp. to operate as a facilities-based and reseller-based carrier under 47 C.F.R. § 63.18(e)(1)-(2) between U.S. and China); Exhibit 12 at EB-408, *Int’l Authorizations Granted*, 16 FCC Rcd. 14695 (2001) (authorizing China Telecommunications Corp. to operate as a facilities-based and resale-based carrier under 47 C.F.R. § 63.18(e)(1)-(2) between the United States and all international locations except for China).

<sup>22</sup> Exhibit 9 at EB-389, *General FAQs*, China Telecom Americas, <https://www.ctamericas.com/faqs> (last visited Feb. 26, 2019).

<sup>23</sup> *See* Exhibit 1 at EB-1, Letter from Yi-jun Tan to DOJ, FBI and DHS (July 17, 2007); *see also* Exhibit 10 at EB-395, 22 FCC Rcd. 15266 (2007) (granting DHS petition to adopt conditions to China Telecom’s Section 214 authorization subject to an LOA); 47 U.S.C. § 214(c) (granting the Commission authority to attach to any Section 214 authorization “such terms and conditions as in its judgment the public convenience and necessity may require.”).

China Telecom leverages its international Section 214 authorizations to provide both regulated and unregulated services as a “one-stop” provider of a “full suite” of communications services.<sup>24</sup> China Telecom offers U.S. customers access to international private line and leased circuits.<sup>25</sup> China Telecom markets its international private line services as providing “[s]afe—highly secure bandwidth for sensitive data.”<sup>26</sup> China Telecom advertises that its international private lines even have a presence “inside key securities exchanges and financial data centers.”<sup>27</sup>

China Telecom also operates a mobile virtual network operator (MVNO) service under the “CTExcel” brand name and resells mobile services directly to retail customers.<sup>28</sup> It targets CTExcel to more than four (4) million Chinese Americans, two (2) million Chinese tourists

---

<sup>24</sup> Exhibit 9 at EB-389, *supra* note 22.

<sup>25</sup> Exhibit 16 at EB-526, *International Private Leased Circuit from China Telecom Americas*, China Telecom Americas, <https://www.ctamericas.com/wp-content/uploads/2018/10/IPLC.pdf> (last visited Feb. 12, 2019); Exhibit 17 at EB-528, *International Ethernet Private Line from China Telecom Americas*, China Telecom Americas, <https://www.ctamericas.com/wp-content/uploads/2018/10/IEPL.pdf> (last visited Feb. 12, 2019); Exhibit 18 at EB-530, *International Private Lines*, China Telecom Americas, <https://www.ctamericas.com/products-services/data-networking/international-private-lines/> (last visited Mar. 4, 2019). China Telecom may provide or re-sell international private lines with its international Section 214 authorizations. *See* 47 C.F.R. §§ 63.22(d), 63.23(c) (authorizing facilities and resale-based international common carriers to provide, *inter alia*, private line, data and business services); *see also Int’l Authorizations Granted*, 20 FCC Rcd. 5985 (2005) (granting authority to make assignment of assets, including private line circuits, from Global Crossing Telecommunications, Inc. to Westcom Corp., where Global Crossing was operating pursuant to international Section 214 authorizations); *In the Matter of Fonorola Corp. & Emi Commc’ns Corp.*, 9 FCC Rcd. 4066 (1994) (discussing an international Section 214 carrier’s provision of facsimile, data, and international message telephone services over resold international private lines) (citation omitted).

<sup>26</sup> Exhibit 16 at EB-527, *supra* note 25; *see also* Exhibit 17 at EB-528, *supra* note 25.

<sup>27</sup> Exhibit 18 at EB-530, *supra* note 25.

<sup>28</sup> Exhibit 22 at EB-542, *CTExcel*, China Telecom Americas, [https://www.ctexcel.us/index\\_pc.jsp?language=en](https://www.ctexcel.us/index_pc.jsp?language=en) (last visited Feb. 26, 2019).

visiting the United States annually, 300,000 Chinese students at U.S. colleges, and more than 1,500 Chinese businesses in the United States.<sup>29</sup>

China Telecom also offers several services for which it is unclear that an international Section 214 authorization is required but could potentially be affected by future FCC actions. China Telecom's existing FCC authorizations provide a level of certainty that allow it to offer enterprise-level services that fall within regulatory "gray areas." Such services include China Telecom's MPLS VPN<sup>30</sup> services to provide global "point-to-point" connections, as well as the ability to "converge [ ] multi-site voice, data, video and cloud applications across locations onto one secure global network."<sup>31</sup> Also included are China Telecom's SD-WAN<sup>32</sup> services to "effectively route traffic from your global offices and data center sites[.]"<sup>33</sup> Another category of services that fall within this "gray area" are virtual private local area network (LAN) services, which provide "worldwide Ethernet connectivity to help enterprises to reduce network cost,

---

<sup>29</sup> Exhibit 23 at EB-547, Press Release, China Telecom Americas, *China Telecom has big US plan* (Jan. 15, 2016), <https://www.ctamericas.com/china-telecom-big-us-plan/>.

<sup>30</sup> MPLS VPN or multi-protocol label switching virtual private networks. MPLS is a mode of communications transport that can carry different kinds of communications, including circuit (traditional telephone) and packet (Internet) communications. VPNs allow users to connect from geographically separate locations to a private network, such as users in different branch offices connecting to one corporate intranet. MPLS VPNs use virtual point-to-point MPLS interconnections to set up VPNs. See Exhibit 20 at EB-535, *MPLS VPN*, China Telecom Americas, <https://www.ctamericas.com/products-services/data-networking/mpls-vpn/> (last visited Feb. 26, 2019).

<sup>31</sup> *Id.* at EB-535-36.

<sup>32</sup> See Exhibit 21 at EB-539, *Software Defined WAN*, China Telecom Americas, <https://www.ctamericas.com/products-services/data-networking/software-defined-wan/> (last visited Feb. 26, 2019). SD-WAN or software-defined wide-area network. SD-WAN is a type of network architecture that allows enterprises to connect geographically separate offices to each other using different modes of communications transport (such as MPLS and broadband).

<sup>33</sup> *Id.* at EB-539.

deploy diversified options and improve connectivity among geographically dispersed locations.”<sup>34</sup>

China Telecom also offers data center and cloud services that do not require an international Section 214 authorization.<sup>35</sup> These services provide customers with “fast, reliable and secure multi-point network connections from their global offices, data centers or colocation environments[.]”<sup>36</sup> China Telecom advertises that its customers have access to over two dozen physical co-location facilities in the United States,<sup>37</sup> where it supplies “24/7 operations, security and support,” as well as equipment to customers so that they can “avoid the cost, complexity and time required to build and manage [their] own facilities.”<sup>38</sup> In addition, it also provides private cloud “infrastructure enabling [customers] to build, monitor and manage [their] individualized cloud service.”<sup>39</sup>

---

<sup>34</sup> Exhibit 19 at EB-533, *Virtual Private LAN Service*, China Telecom Americas, <https://www.ctamericas.com/wp-content/uploads/2018/10/VPLS-Brochure.pdf> (last visited Feb. 26, 2019). Virtual private LAN service is a way to provide Ethernet-based multipoint to multipoint communication over Internet Protocol (IP) or MPLS.

<sup>35</sup> See, e.g., *China Mobile Order*, 34 FCC Rcd. at 3364 ¶ 4.

<sup>36</sup> Exhibit 27 at EB-558, *Public Cloud Exchange*, China Telecom Americas, <https://www.ctamericas.com/public-cloud-exchange/> (last visited Mar. 1, 2019).

<sup>37</sup> Exhibit 6 at EB-296-331, *Global Data Center Map*, China Telecom Americas, <https://www.ctamericas.com/global-data-center-map/> (last visited Feb. 1, 2019) (showing compiled list of China Telecom’s U.S. Points of Presence, colocation facilities, and cloud exchanges).

<sup>38</sup> Exhibit 28 at EB-561, *Colocation Services*, China Telecom Americas, <https://www.ctamericas.com/products-services/cloud-data-centers/idc-colocation/> (last visited Mar. 1, 2019); see also Exhibit 6 at EB-296, *supra* note 37.

<sup>39</sup> Exhibit 29 at EB-565, *Cloud Infrastructure*, China Telecom Americas, <https://www.ctamericas.com/products-services/cloud-data-centers/enterprise-cloud-services/> (last visited Mar. 1, 2019).

China Telecom is also a managed service provider (MSP). It advertises a “Managed Security” service with “proven security solutions” to “protect . . . mission-critical applications, data and user networks[.]”<sup>40</sup> It also offers “Managed WAN”<sup>41</sup> services, through which it proposes to manage private corporate intranets. This service “enables multi-national organizations to connect . . . to multiple sites via a secure, private and high-performance network.”<sup>42</sup> A “[m]anaged Customer Premises Equipment (CPE) solution” helps U.S. customers outsource their “router and equipment management.”<sup>43</sup>

China Telecom’s existing authorizations include facilities-based authorizations<sup>44</sup> that give China Telecom the option to expand its U.S. presence without needing further FCC approvals. With its current authorizations, China Telecom can continue to extend its existing network,<sup>45</sup> install new equipment or upgrade existing equipment on its network,<sup>46</sup> request additional

---

<sup>40</sup> Exhibit 31 at EB-572, *Managed Security*, China Telecom Americas, <https://www.ctamericas.com/products-services/managed-spervices/managed-security/> (last visited Mar. 1, 2019).

<sup>41</sup> Exhibit 25 at EB-553, *Managed WAN*, China Telecom Americas, <https://www.ctamericas.com/products-services/managed-services/managed-wan/> (last visited Feb. 28, 2019). See also Exhibit 26 at EB-556, *ICT Services*, China Telecom Americas, <https://www.ctamericas.com/wp-content/uploads/2018/10/ICT-Services.pdf> (last visited Feb. 12, 2019). WAN, or wide area network, connects geographically disparate locations onto one private network, such as a corporate intranet.

<sup>42</sup> Exhibit 25 at EB-553, *supra* note 41.

<sup>43</sup> Exhibit 30 at EB-569, *Managed CPE*, China Telecom Americas, <https://www.ctamericas.com/products-services/managed-services/managed-cpe/> (last visited Mar. 1, 2019).

<sup>44</sup> See Exhibit 11 at EB-400, *supra* note 21; and Exhibit 12 at EB-408, *supra* note 21 (China Telecom’s 2001 and 2002 authorizations to operate as facilities-based carrier between the United States and foreign points).

<sup>45</sup> See 47 C.F.R. § 63.02(a) (2018) (“Any common carrier is exempt from the requirements of Section 214 . . . for the extension of any line.”).

<sup>46</sup> See 47 U.S.C. § 214(a) (“[N]othing in this section shall be construed to require a

interconnections with the networks of other U.S. common carriers,<sup>47</sup> or provide facilities-based mobile wireless services using its own network facilities instead of reselling mobile services as it currently does as an MVNO<sup>48</sup>—all without seeking further FCC approvals under Section 214. As explained in the next section, the potential for China Telecom to increase its capabilities as a common carrier heightens the national security and law enforcement concerns raised in this recommendation.

**IV. The Executive Branch recommends revocation and termination of China Telecom’s international Section 214 authorizations**

Under Section 214 of the Communications Act, a carrier may not provide common carrier telecommunications services without first obtaining from the Commission a certificate that the “present or future public convenience and necessity require” those services.<sup>49</sup> The Commission considers a number of factors in evaluating relevant public interest concerns, including national security, law enforcement, foreign policy, and trade concerns raised by the Executive Branch.<sup>50</sup>

---

certificate or other authorization from the Commission for any installation, replacement, or other changes in plant, operation, or equipment, other than new construction, which will not impair the adequacy or quality of service provided.”).

<sup>47</sup> See *China Mobile Order*, 34 FCC Rcd. at 3377 ¶ 33 n.98 (finding that with an international Section 214 authorization, China Mobile would be able to request interconnection with the networks of other Section 214-authorized U.S. common carriers).

<sup>48</sup> See *id.* at 3364 ¶ 4 n.20; see also *id.* at 3377 ¶ 33 n.98 (finding that China Mobile would need an international Section 214 authorization to transport communications from the United States to foreign points as an MVNO operator).

<sup>49</sup> 47 U.S.C. § 214(a) (emphases added).

<sup>50</sup> See *In the Matter of Mkt. Entry & Regulation of Foreign-Affiliated Entities*, 11 FCC Rcd. 3873, ¶ 3, 3897 ¶ 62 (1995) (*First Foreign Participation Order*).

When it comes to national security and law enforcement concerns, an applicant for an international Section 214 authorization is not entitled to a presumption that its application is in the public interest.<sup>51</sup> The FCC has stated that although an applicant for an international Section 214 authorization may be entitled to a rebuttable presumption that grant of its application would not be contrary to the public interest—on competition grounds—no such presumption applies to national security and law enforcement concerns.<sup>52</sup> The applicant has the burden to show that the public interest would be served by the grant despite national security and law enforcement risks identified by the Executive Branch.<sup>53</sup> The Commission “accord[s] deference to the expertise of the Executive Branch in identifying and interpreting issues of concern related to national security, law enforcement, and foreign policy” relevant to a pending Section 214 application.<sup>54</sup> Because Section 214(a) directs the Commission to act when “present” or “future” interests are concerned, and to determine whether the public convenience and necessity “require” the carrier’s services,<sup>55</sup> the Commission should also apply the same deference to the Executive Branch’s expertise with respect to any national security and law enforcement concerns associated with an existing international Section 214 authorization.

---

<sup>51</sup> See *In the Matter of Rules & Policies on Foreign Participation in the U.S. Telecommunications Mkt.*, 12 FCC Rcd. 23891, 23920 ¶ 65 (1997) (*Second Foreign Participation Order*).

<sup>52</sup> *China Mobile Order*, 34 FCC Rcd. at 3367 ¶ 11.

<sup>53</sup> *Id.*

<sup>54</sup> *Second Foreign Participation Order*, 12 FCC Rcd. at 23920 ¶ 63.

<sup>55</sup> 47 U.S.C. § 214(a).

The Executive Branch, and specifically DOJ, DHS, and DoD (collectively, Team Telecom<sup>56</sup>), reviews international Section 214 carrier authorizations for national security and law enforcement concerns. In *China Mobile*, Team Telecom publicly disclosed a multifactor analysis it applies when making a recommendation based on national security and law enforcement concerns.<sup>57</sup> These factors include, but are not limited to:

The Carrier:

1. Whether the carrier has a past criminal history;
2. Whether the carrier has engaged in conduct that calls the carrier's trustworthiness into question; and
3. Whether the carrier is vulnerable to exploitation, influence, or control by other actors;

State Control, Influence and Ability to Compel Carrier to Provide Information:

4. Whether the carrier's foreign ownership could result in control of U.S. telecommunications infrastructure or persons operating such infrastructure by a foreign government or an entity controlled by or acting on behalf of a foreign government;
5. Whether the carrier's foreign ownership is from a country suspected of engaging in actions, or possessing the intention to take actions, that could impair U.S. national security;
6. Whether the carrier will be required, by virtue of its foreign ownership, to comply with foreign requests (e.g., requests for communications intercepts) relating to the carrier's operations within the United States, or whether the carrier is otherwise susceptible to such requests and/or demands made by a foreign nation or other actors; and
7. Whether such requests are governed by publicly available legal procedures subject to independent judicial oversight;

The Carrier's U.S. Operations:

8. Whether the carrier's operations within the United States provide opportunities for the carrier or other actors to undermine the reliability of the domestic communications infrastructure;
9. Whether the carrier's operations within the United States provide opportunities for the carrier or other actors to identify and expose national security vulnerabilities;

---

<sup>56</sup> See *Second Foreign Participation Order*, 12 FCC Rcd. at 23919 ¶ 62 (The Team Telecom agencies consist of the "federal agencies [that] have specific expertise" on national security and law enforcement issues and lead the Executive Branch's assessment on those issues.).

<sup>57</sup> Redacted Executive Branch Recommendation to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization, FCC No. ITC-214-20110901-00289, at 6-7 (filed July 2, 2018), [https://licensing.fcc.gov/myibfs/download.do?attachment\\_key=1444739](https://licensing.fcc.gov/myibfs/download.do?attachment_key=1444739).



10. Whether the carrier's operations within the United States provide opportunities for the carrier or other actors to render the domestic communications infrastructure otherwise vulnerable to exploitation, manipulation, attack, sabotage, or covert monitoring;
11. Whether the carrier's operations within the United States provide opportunities for the carrier or other actors to engage in economic espionage activities against corporations that depend on the security and reliability of the U.S. communications infrastructure to engage in lawful business activities; or
12. Whether the carrier's operations within the United States provide opportunities for the carrier or other actors to otherwise engage in activities with potential national security implications;

Requirements of U.S. Legal Process:

13. Whether the Executive Branch will be able to continue to conduct its statutorily authorized law enforcement and national security missions, which may include issuance of legal process for the production of information or provision of technical assistance; including
14. Whether the confidentiality requirements that protect information about the targets of lawful surveillance and classified sources and methods will continue to be effective.

(collectively, the Factors).<sup>58</sup> Team Telecom developed the Factors based on input from agencies with expertise in national security and law enforcement matters, as well as past experiences evaluating applications referred by the Commission and monitoring the effectiveness of mitigation measures.

Team Telecom, as the expert agencies within the Executive Branch for identifying and addressing national security and law enforcement concerns, publicly applied these Factors for the first time in the July 2018 recommendation to deny China Mobile International (USA) Inc.'s application for an international Section 214 authorization.<sup>59</sup> China Telecom's ongoing operations in the United States raise similar—but more pressing—national security and law enforcement concerns. Accordingly, Team Telecom applied the same Factors in the Executive Branch's recommendation herein that the Commission revoke and terminate China Telecom's

---

<sup>58</sup> *Id.* at 6-7.

<sup>59</sup> *See id.*; *see also* *China Mobile Order*, 34 FCC Rcd. at 3368 ¶ 14 n.46, 3367 ¶ 12, and 3374 ¶ 26 (citing the Factors in denying China Mobile's application for an international Section 214 authorization).

existing international Section 214 authorizations.

In light of the current national security environment, the Executive Branch has determined that 13 of the 14 Factors weigh strongly in favor of revocation and termination. Only the first Factor, China Telecom's lack of criminal history, is neutral. The Executive Branch's recommendation considered:

- China Telecom's past conduct, which includes making inaccurate statements to Team Telecom about where it stored U.S. records, making inaccurate statements to U.S. customers about its cybersecurity practices, and potentially failing to comply with U.S. federal and state cybersecurity and privacy laws (Factor 2);
- The Chinese government's ultimate ownership and control of China Telecom, and the Chinese Communist Party's (CCP) recently strengthened influence and control over China Telecom's parent entity (Factors 3-4);
- China Telecom's forced compliance with Chinese government requests (Factors 6-7);
- China Telecom's operations in the United States, which provide opportunities for increased Chinese government-sponsored economic espionage, theft of trade secrets (Factors 5, 9-12), and the disruption and misrouting of U.S. communications traffic (Factors 5, 8-10, 12); and
- China Telecom's lack of trustworthiness, which limits the Executive Branch's ability to conduct statutorily authorized law enforcement and national security missions and effectively protect information about investigations and classified sources and missions (Factors 13-14).

**A. China Telecom has engaged in conduct that calls its trustworthiness into question (Factor 2)<sup>60</sup>**

Team Telecom, while monitoring China Telecom's LOA compliance over the past year, has discovered conduct that calls into question China Telecom's trustworthiness. This includes China Telecom's 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 and state cybersecurity and privacy laws.

As an initial matter, China Telecom 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. In June 2018, Team Telecom asked for copies of China Telecom's cybersecurity policies in order to monitor compliance with the LOA's requirement that China Telecom "take all practicable measures" to prevent unauthorized access to U.S. Records.<sup>61</sup> China Telecom did not immediately disclose that [REDACTED]

Instead, it delayed its response for six months, during which Team Telecom repeated its request five more times.<sup>62</sup> In December 2018, China Telecom produced two documents, neither of

---

<sup>60</sup> Factor 2 considers whether a carrier has engaged in conduct that calls its trustworthiness into question.

<sup>61</sup> See Business Confidential Exhibit 32 at EB-576, Letter from DOJ National Security Division to China Telecom (June 13, 2018) (citing LOA).

<sup>62</sup> See Business Confidential Exhibit 33 at EB-578, E-mail from Morgan, Lewis & Bockius (hereinafter Morgan Lewis), China Telecom's outside counsel, to DOJ National Security Division (Aug. 30, 2018) (DOJ's first follow-up e-mail on July 23, 2018 and second follow-up e-mail on August 29, 2018); Business Confidential Exhibit 34 at EB-581, E-mail from Morgan Lewis to DOJ National Security Division (Sept. 18, 2018) (DOJ's third follow-up e-mail on September 17, 2018); Business Confidential Exhibit 35 at EB-587, EB-586, E-mail from Morgan Lewis to DOJ National Security Division (Nov. 26, 2018) (DOJ's fourth follow-up e-mail on November 6, 2018; DOJ's fifth follow-up e-mail on Nov. 15, 2018).

which existed when Team Telecom made the initial request. The first document, [REDACTED] [REDACTED] was dated five days before China Telecom provided it to Team Telecom.<sup>63</sup> The second, [REDACTED] [REDACTED] [REDACTED] was improperly redacted and dated one month before China Telecom provided it to Team Telecom.<sup>64</sup> [REDACTED]

[REDACTED]

After further negotiation, China Telecom disclosed that the redaction concealed [REDACTED] [REDACTED] [REDACTED] [REDACTED]

Aside from the delays, the Executive Branch is troubled by new disclosures in these documents that indicate China Telecom made inaccurate statements to U.S. government authorities about where it stored U.S. records and to U.S. customers about its cybersecurity

---

<sup>63</sup> See Business Confidential Exhibit 36 at EB-593, Letter from Morgan Lewis to DOJ National Security Division with attachments (Dec. 6, 2018) [REDACTED]

<sup>64</sup> *Id.* at EB-621.

<sup>65</sup> Business Confidential Exhibit 37 at EB-655, E-mail from Morgan Lewis to DOJ National Security Division (Jan. 24, 2019).

practices. China Telecom's inadequate cybersecurity and privacy practices raise questions as to whether it has complied with relevant federal and state laws.

1. China Telecom made inaccurate statements to Team Telecom about where it stored U.S. records

China Telecom's recent disclosures indicate that China Telecom previously made inaccurate statements to Team Telecom about where it stored U.S. records. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] After further questioning by Team Telecom, China Telecom admitted that [REDACTED]

[REDACTED]

[REDACTED]

This admission contradicts China Telecom's January 2016 statement that [REDACTED]

[REDACTED]

[REDACTED] China Telecom previously represented to Team Telecom that [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>66</sup> Business Confidential Exhibit 36 at EB-624. *supra* note 63. [REDACTED]

[REDACTED]

<sup>67</sup> Business Confidential Exhibit 103 at EB-2111-2112, Letter from Morgan Lewis to DOJ National Security Division (April 4, 2019) [REDACTED]

[REDACTED]

<sup>68</sup> Business Confidential Exhibit 125 at EB-2784, Letter from China Telecom to DOJ, FBI, and DHS (Jan. 11, 2016).

[REDACTED]

[REDACTED]

[REDACTED] China Telecom has not explained the apparent contradiction in its January 11, 2016 and April 4, 2019 letters to Team Telecom.

When Team Telecom attempted to investigate further and requested access logs of foreign access to China Telecom's U.S. customer records, China Telecom claimed that it

[REDACTED]

[REDACTED]

---

<sup>69</sup> *Id.*

<sup>70</sup> Business Confidential Exhibit 103 at EB-2113, *supra* note 67.

<sup>71</sup> Business Confidential Exhibit 36 at EB-624, *supra* note 63.

[REDACTED]

<sup>72</sup> Business Confidential Exhibit 103 at EB-2112, *supra* note 67; *see also* Business Confidential Exhibit 119 at EB-2745, Letter from DOJ National Security Division to Morgan Lewis (May 29, 2019).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Team Telecom, through DOJ, FBI, and DHS, relied on this representation when, two months later, it recommended that the FCC grant international Section 214 authorizations to China Telecom subject to the 2007 LOA.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

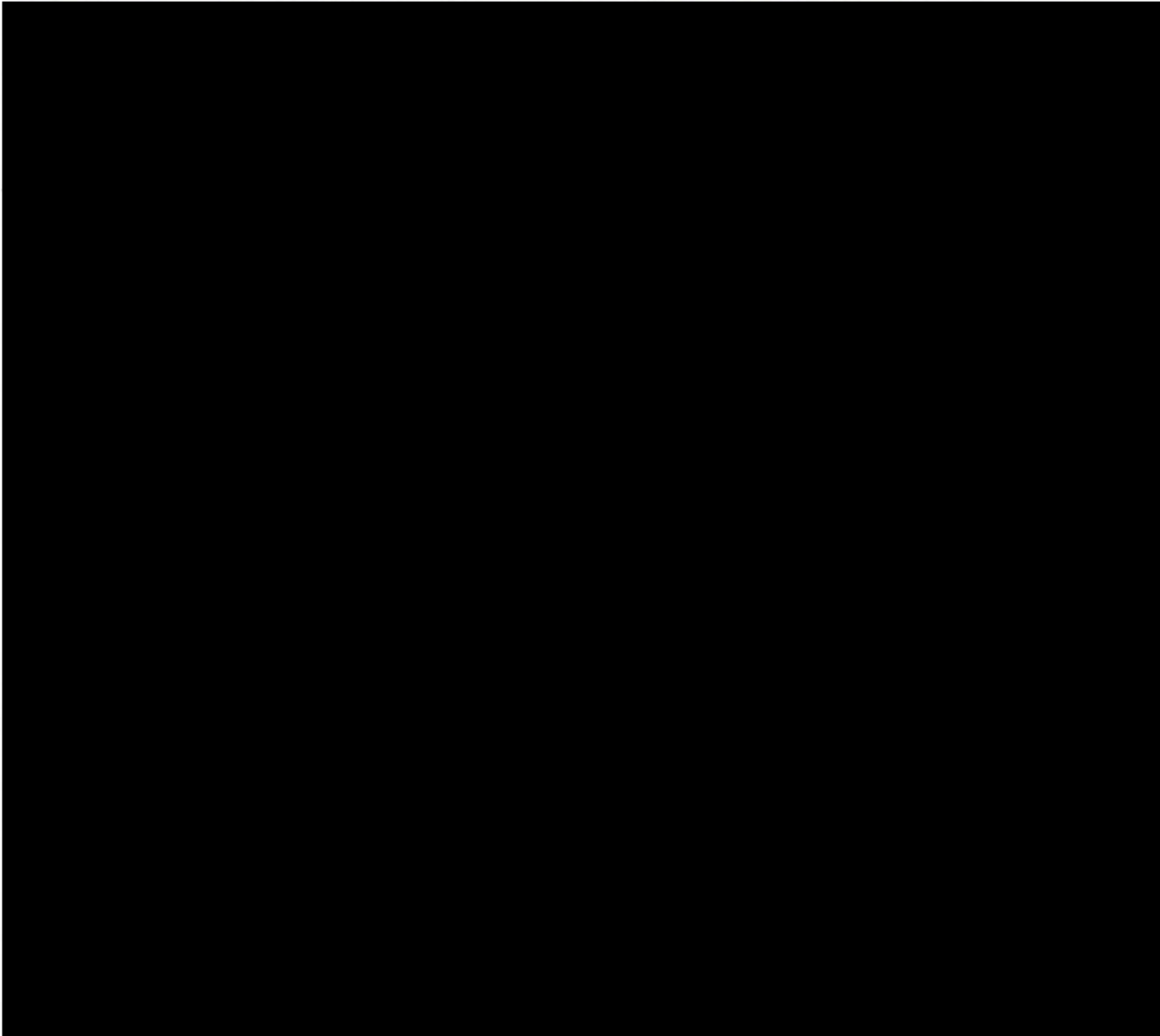
[REDACTED]

[REDACTED]

---

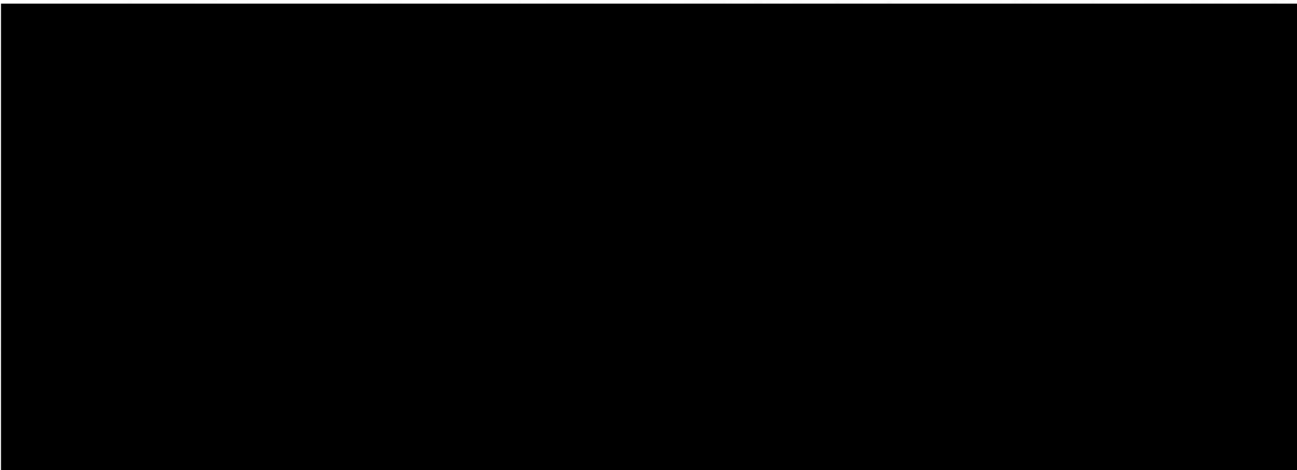
<sup>73</sup> Business Confidential Exhibit 3 at EB-15, Responses of China Telecom to Combined Questions for FCC Applicants, dated May 11, 2007 (emphasis added).

<sup>74</sup> Business Confidential Exhibit 36 at EB-621, *supra* note 63.

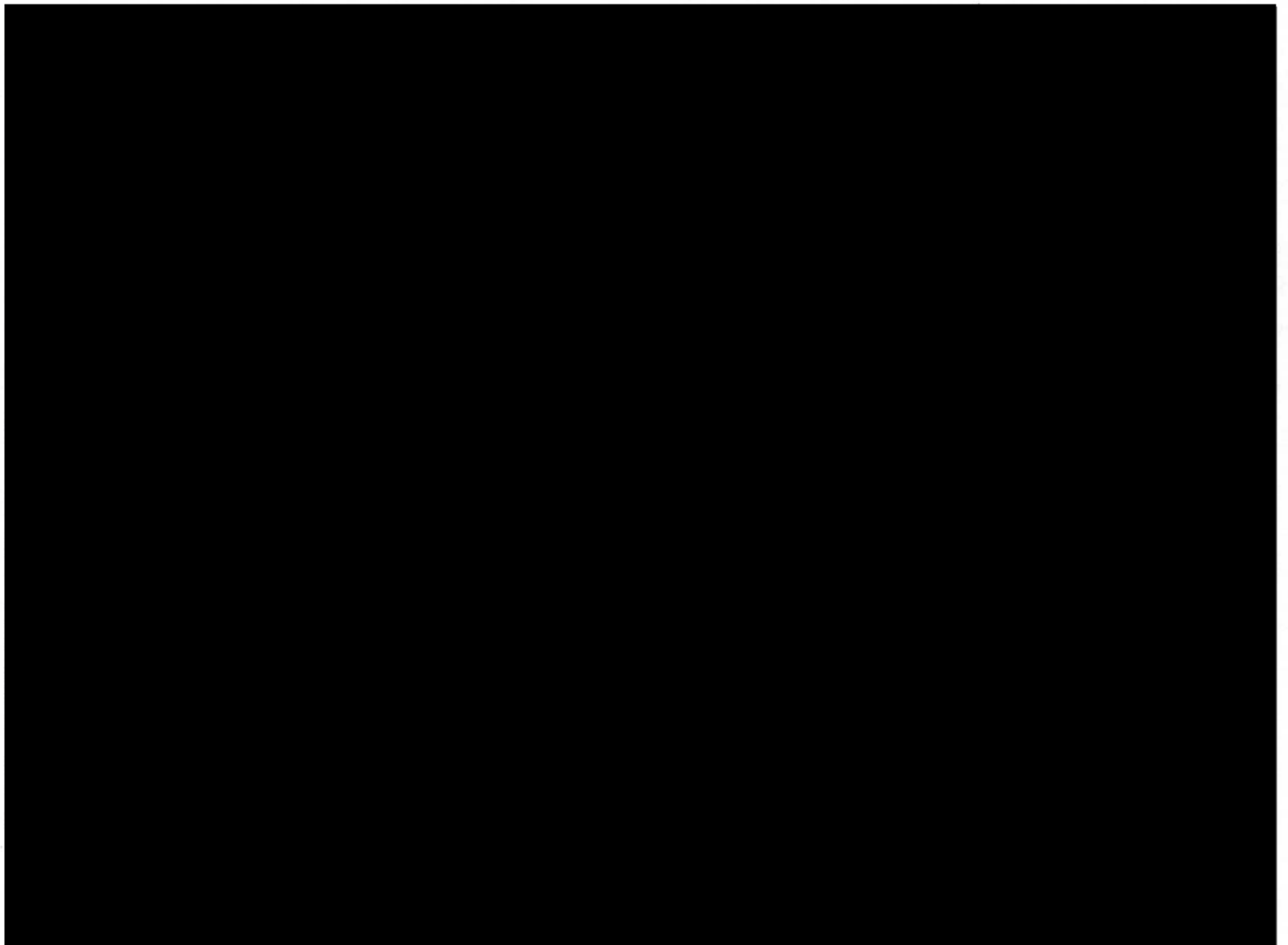
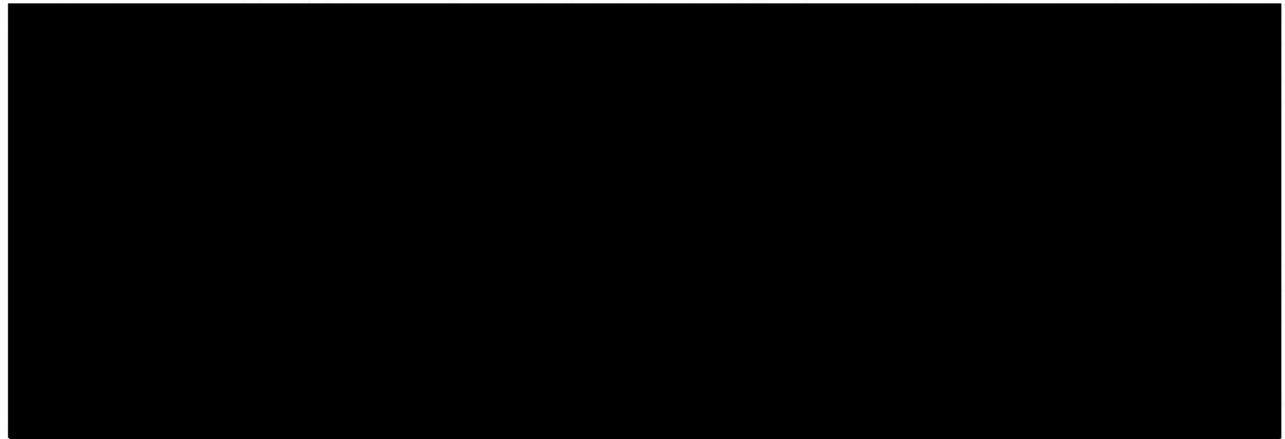


---

<sup>75</sup> *Id.*







---

<sup>78</sup> *Id.* at EB-634.

<sup>79</sup> *Id.*

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED] China

Telecommunications Corporation is China Telecom's ultimate parent entity, and is directly under Chinese government supervision; it owns 70.89 percent of the Parent Entity (CTCL), which in turn wholly owns both CTG and China Telecom.<sup>83</sup> [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]

---

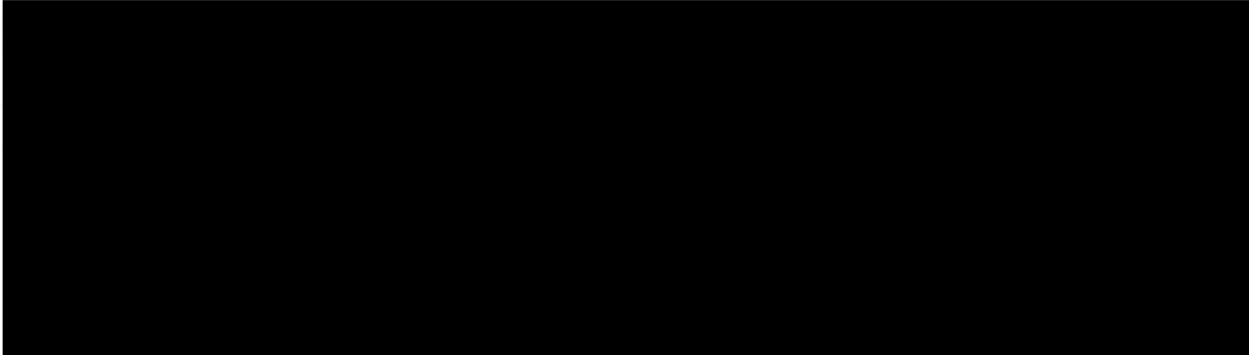
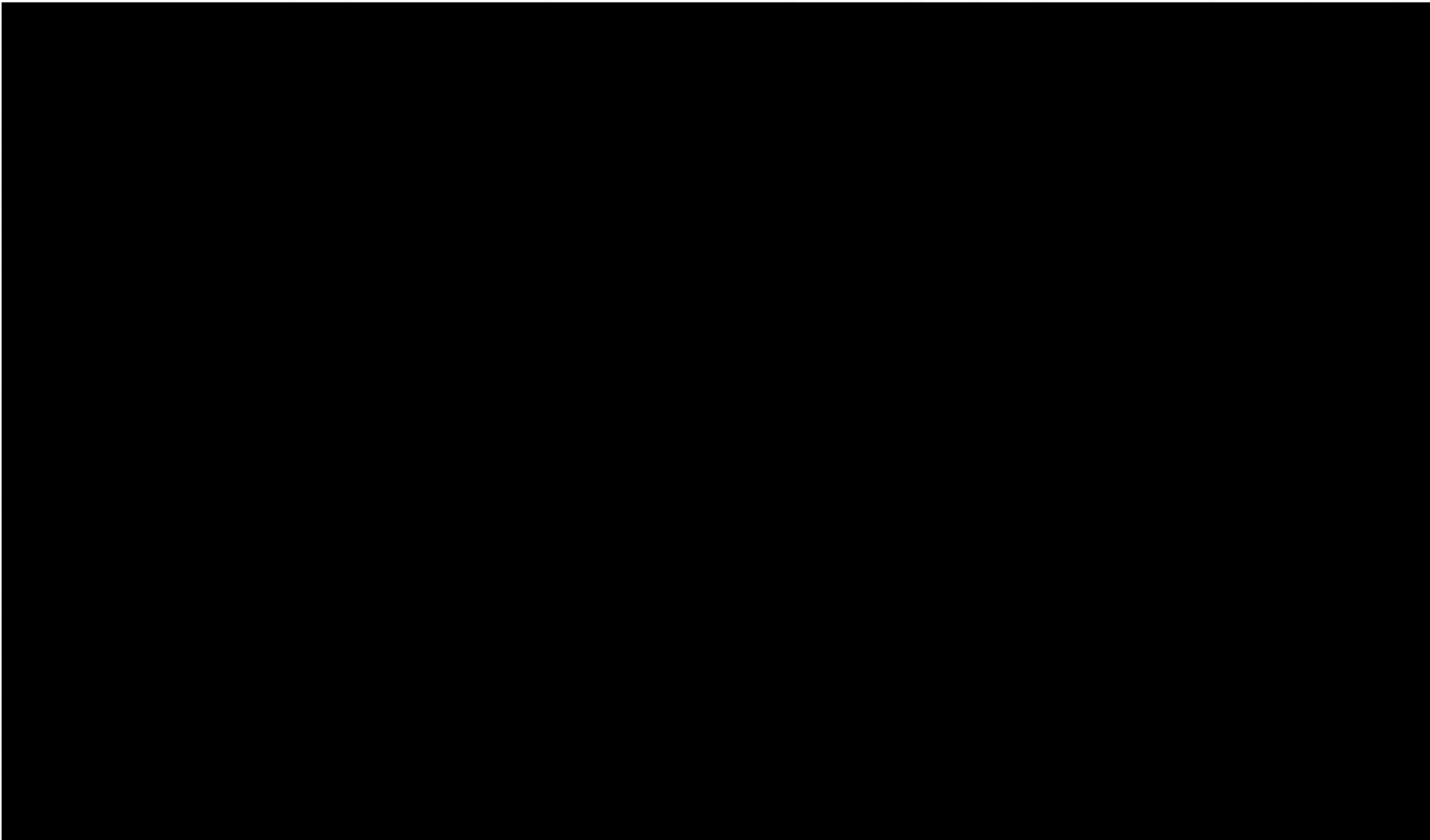
<sup>80</sup> Business Confidential Exhibit 103 at EB-2112, *supra* note 67 [REDACTED]  
[REDACTED]

<sup>81</sup> Business Confidential Exhibit 36 at EB-622, *supra* note 63 [REDACTED]  
[REDACTED] *see*  
*also* Business Confidential Exhibit 103 at EB-2113, *supra* note 67.

<sup>82</sup> Business Confidential Exhibit 103 at EB-2111, *supra* note 67 (response to Question No. 7).

<sup>83</sup> Exhibit 4 at EB-67, China Telecom Corp. Ltd., Annual Report Form 20-F (Apr. 27, 2018) (ownership chart).

<sup>84</sup> The ownership diagram is derived from information in Exhibit 4 at EB-67, *supra* note 83. [REDACTED]  
[REDACTED]



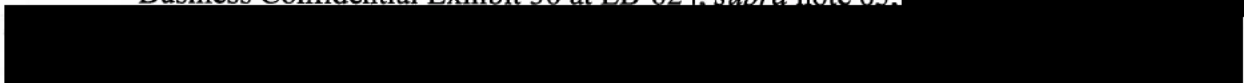
Until questioned by Team Telecom in March 2019, China Telecom did not correct its inaccurate statement that [REDACTED]



---

<sup>85</sup> Business Confidential Exhibit 103 at EB-2113, *supra* note 67.

<sup>86</sup> Business Confidential Exhibit 36 at EB-624, *supra* note 63.



[REDACTED]

[REDACTED] Such conduct calls China Telecom's trustworthiness into question and significantly undermines Team Telecom's and the Executive Branch's confidence in any ability to mitigate the national security and law enforcement concerns associated with China Telecom's FCC authorizations.

2. China Telecom made inaccurate statements to U.S. customers about its cybersecurity practices and may have failed to comply with U.S. cybersecurity and privacy laws

The Executive Branch also learned that [REDACTED]

[REDACTED]

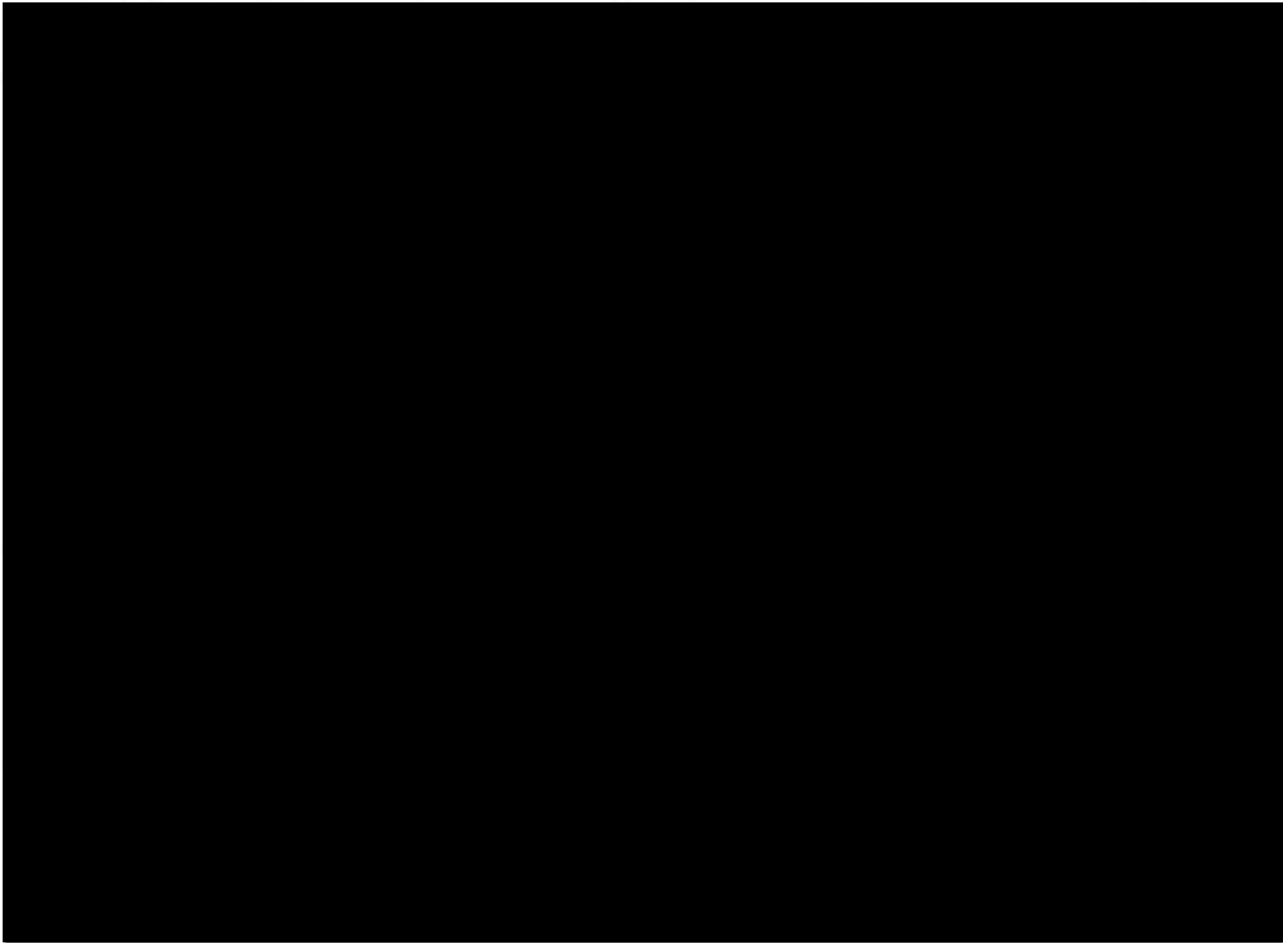
[REDACTED] Having failed to respond substantively to Team Telecom's June 2018 request for cybersecurity policies for six months, China Telecom finally submitted what it described as

[REDACTED]

---

<sup>87</sup> *Id.* at EB-590 (emphasis added).

<sup>88</sup> Business Confidential Exhibit 37 at EB-655, *supra* note 65.



Even if China Telecom had [REDACTED]  
[REDACTED] it has provided no evidence that it complies  
with its existing policies. [REDACTED]

---

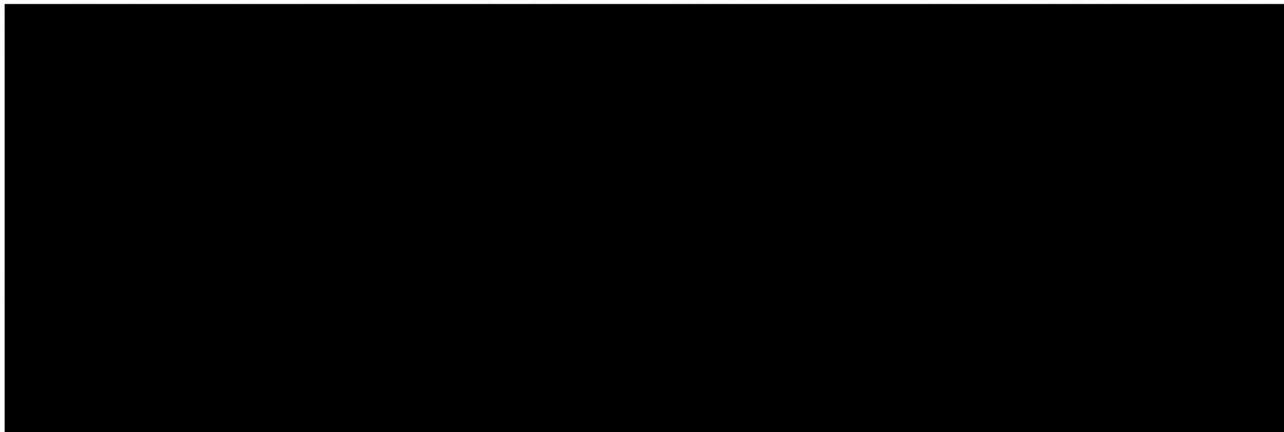
<sup>89</sup> Business Confidential Exhibit 102 at EB-2103, Letter from DOJ National Security Division to Morgan Lewis (Mar. 21, 2019) (quoting Exhibit 1 at EB-2, *supra* note 23).

<sup>90</sup> Business Confidential Exhibit 103 at EB-2107, *supra* note 67.

<sup>91</sup> *Id.* at EB-2108; *see also* Business Confidential Exhibit 119 at EB-2745, *supra* note 72.

<sup>92</sup> Business Confidential Exhibit 103 at EB-2108, EB-2112-13, *supra* note 67.

<sup>93</sup> Business Confidential Exhibit 119 at EB-2745, *supra* note 72 (summarizing May 21, 2019 meeting between China Telecom and Team Telecom); *see also* Business Confidential Exhibit 124 at EB-2774, Letter from Morgan Lewis to DOJ National Security Division (June 14, 2019).



First, China Telecom's [REDACTED]

[REDACTED] may potentially run afoul of federal law. China Telecom may have let customers believe that they would receive a higher level of cybersecurity than they actually did. China Telecom promised its customers “maximum security,”<sup>95</sup> and enticed them to trust China Telecom with their “mission-critical” data.<sup>96</sup> China Telecom specifically targeted these claims to U.S. customers operating in the financial, logistics, retail, energy, media, and healthcare industries.

---

<sup>94</sup> Business Confidential Exhibit 36 at EB-624. *supra* note 63. [REDACTED]

<sup>95</sup> Exhibit 38 at EB-659, *Developing a Trusted Security Strategy for China*, China Telecom Americas, <https://www.ctamericas.com/developing-security-strategy-for-china/> (last visited Mar. 23, 2019) (advertising the “CTA [China Telecom] difference” is “providing maximum security”).

<sup>96</sup> Exhibit 31 at EB-572, *supra* note 40.



(Above: Excerpted from Exhibit 42 at EB-699, emphasis in red).<sup>97</sup>

The Federal Trade Commission (FTC) has previously found statements made under similar circumstances to be unfair and deceptive practices under Section 5(a) of the Federal Trade Commission Act (FTCA).<sup>98</sup> In 2016, the FTC sued the operators of the AshleyMadison.com website, alleging that the defendants misrepresented their network security to customers; the FTC specifically cited AshleyMadison.com’s failure “to have a written organizational information security policy.”<sup>99</sup> China Telecom’s [REDACTED]

[REDACTED] while advertising “maximum security” for its data and telecommunications

<sup>97</sup> Exhibit 42 at EB-699, *Financial*, China Telecom Americas, <https://www.ctamericas.com/industry-solutions/financial> (last visited Feb. 15, 2019).

<sup>98</sup> 15 U.S.C. § 45(a).

<sup>99</sup> Exhibit 40 at EB-668, *Federal Trade Comm’n v. Ruby Corp.*, Case No. 16-cv-2438, Dkt. No. 1, Complaint at ¶ 31, 43-47 (D.D.C. filed Dec. 14, 2016). The defendants settled the FTC’s complaint by stipulating to a permanent injunction against misrepresenting security practices and agreeing to a partially suspended monetary judgment of \$8.75 million. See Exhibit 41 at EB-684, *Federal Trade Comm’n v. Ruby Corp.*, Case No. 16-cv-2438, Dkt. 9, Stipulated Order for Permanent Injunction and Other Equitable Relief (D.D.C. Dec. 19, 2016).

services, raises questions about whether China Telecom and its Parent Entity have complied with federal laws such as Section 5(a) of the FTCA.

*Second*, China Telecom's [REDACTED]

[REDACTED] raises questions about whether it complied with more specific state laws requiring formal cybersecurity policies and appropriate data protection practices. These laws include:

- Ohio law requiring businesses to “create, maintain, and comply with a written cybersecurity program” to avoid liability for unreasonable information security practices.<sup>100</sup> China Telecom is subject to Ohio law because it has engaged in sales and business development in Ohio.<sup>101</sup>
- Colorado law requiring businesses to “implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations.”<sup>102</sup> China Telecom is subject to Colorado law because it has a Point of Presence in Denver, Colorado.<sup>103</sup>
- Delaware law requiring any business that “owns, licenses or maintains personal information [to] implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of

---

<sup>100</sup> See Ohio Rev. Code Ann. § 1354.02 (West, 2018) (requiring written cybersecurity program to qualify for an affirmative defense).

<sup>101</sup> See Exhibit 84 at EB-1928, Xiruo Zhao, LinkedIn, <https://www.linkedin.com/in/xiruo-zhao-361a9bb7/>. (last visited Mar. 12, 2019) (disclosing 650+ China Telecom sim card sales in Ohio in 2018).

<sup>102</sup> Colo. Rev. Stat. § 6-1-713.5(1) (2018).

<sup>103</sup> See Exhibit 6 at EB-296, EB-302, *supra* note 37 (Coresite DE1 PoP in Denver, CO).



personal information.”<sup>104</sup> China Telecom is subject to Delaware law because it is incorporated in Delaware.<sup>105</sup>

- California law requiring businesses to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.”<sup>106</sup> China Telecom is subject to California law because it maintains a Global Network Operations Center (NOC)<sup>107</sup> and significant facilities in California.<sup>108</sup>

California law enacted in 2004 also requires businesses to post privacy policies “conspicuously” on their websites.<sup>109</sup> According to China Telecom, [REDACTED]  
[REDACTED]  
[REDACTED] As late as July 2, 2017, a publicly available cached version of China Telecom’s website site map did not show a link to a privacy policy.<sup>111</sup> China Telecom’s apparent failure to comply with California’s

---

<sup>104</sup> Del. Code § 12B-100 (2018).

<sup>105</sup> Exhibit 2 at EB-4, China Telecom (USA) Corporation Stock Purchase Agreement (June 15, 2007).

<sup>106</sup> Cal. Civ. Code § 1798.81.5(b) (West, 2018).

<sup>107</sup> Exhibit 85 at EB-1936, *Office Locations*, China Telecom Americas, <https://www.ctamericas.com/office-locations/> (last visited Mar. 13, 2019).

<sup>108</sup> Exhibit 6 at EB-296, EB-304-311, EB-318, EB-320-27, *supra* note 37.

<sup>109</sup> Cal. Bus. & Prof. Code § 22575 (West, 2018).

<sup>110</sup> Business Confidential Exhibit 103 at EB-2113, *supra* note 67.

<sup>111</sup> Exhibit 43, *Site Map*, China Telecom Americas, cached July 2, 2017, <https://web.archive.org/web/20170702035054/>, <http://www.ctamericas.com/sitemap/> (last visited

privacy policy law is exacerbated by the fact that China Telecom has maintained significant operations in California since at least 2004.<sup>112</sup>

While any one of these omissions and violations might be excused as an oversight, collectively they demonstrate a corporate disregard for regulations designed to protect the privacy and security of Americans' data. An FCC Section 214 authorization empowering the collection, storage, and transport of such data by such an entity is not in the public interest.

**B. China Telecom is owned and controlled by Chinese parent entities and ultimately by the Chinese government (Factors 3 and 4)<sup>113</sup>**

As the wholly owned subsidiary of a parent entity that is majority-owned by a Chinese state-owned enterprise, China Telecom is ultimately owned and controlled by the Chinese government. China Telecom's parent, China Telecom Corp. Ltd. (CTCL, or the Parent Entity), is a Chinese company that has over \$50 billion in assets, employs more than 371,000 professionals, and manages 70 percent of the Internet in China.<sup>114</sup> The Parent Entity is majority-owned (70.89 percent) through an intermediary (China Telecommunications Corp., also known as China Telecom Group) owned by the State-owned Assets Supervision and Administration Commission (SASAC) of the State Council of China.<sup>115</sup> In addition to the Chinese government's

---

Apr. 2, 2019) (showing China Telecom Americas website sitemap with no record of a privacy policy on July 2, 2017).

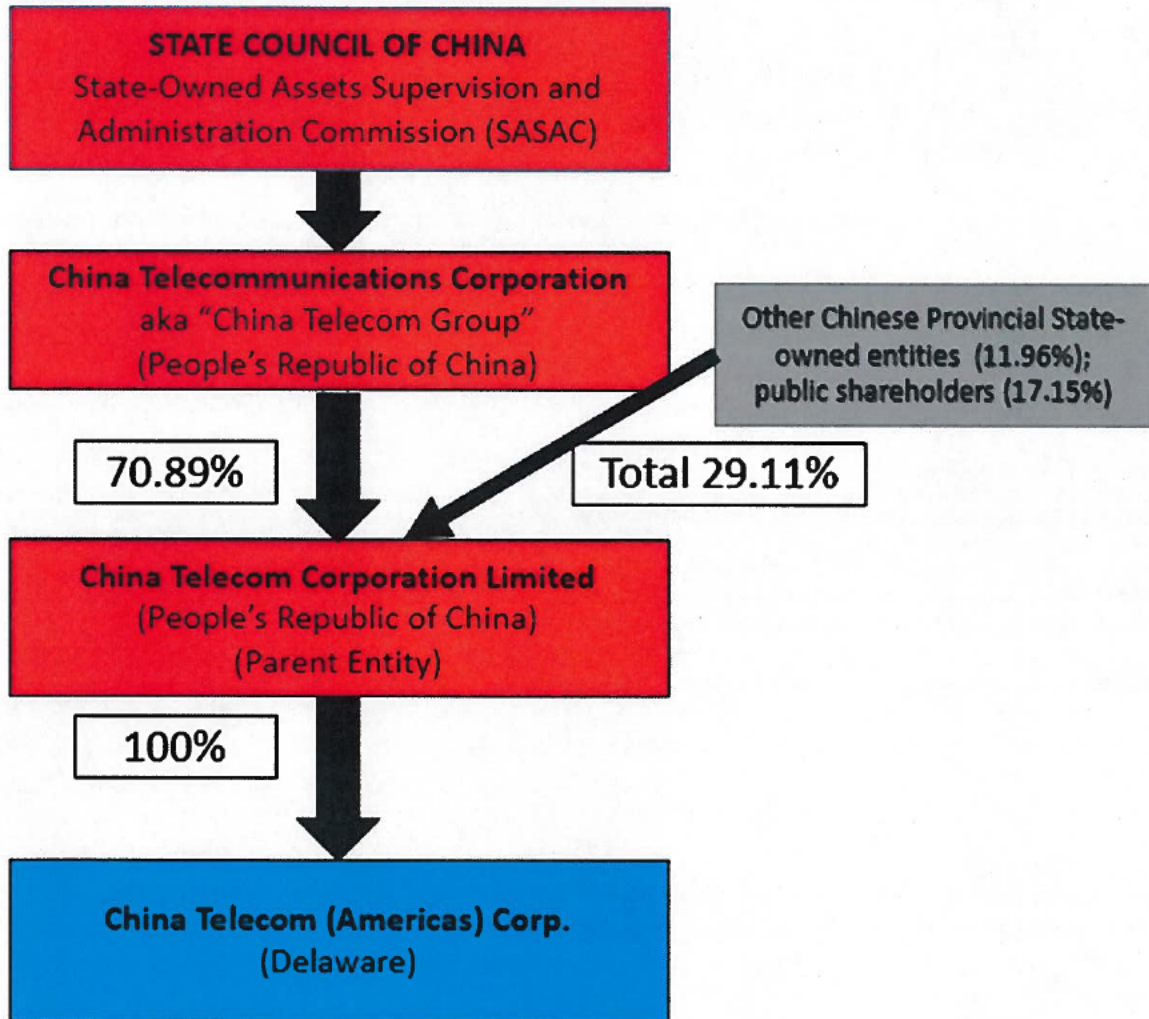
<sup>112</sup> Exhibit 9 at EB-389, *supra* note 22.

<sup>113</sup> Factor 3 considers whether the carrier is vulnerable to exploitation, influence or control by other actors. Factor 4 considers whether the carrier's foreign ownership could result in control of U.S. telecommunications infrastructure or persons operating such infrastructure by a foreign government or an entity controlled by or acting on behalf of a foreign government.

<sup>114</sup> Exhibit 9 at EB-389-90, *supra* note 22.

<sup>115</sup> Exhibit 4 at EB-32, EB-42, EB-67, *supra* note 83.

70.89 percent ownership, Chinese provincial state-owned entities own 11.96 percent,<sup>116</sup> for a combined 82.85 percent ownership by all Chinese government entities. China Telecom’s relevant ownership is illustrated in the diagram<sup>117</sup> below:



Factors 3 and 4, applied to these facts, weigh strongly in favor of revocation and termination. The Commission previously considered similar factors in *China Mobile* to support

<sup>116</sup> *Id.* at EB-67. The provincial state-owned entities are Guangdong Rising Assets Management Co., Ltd. (6.94 percent), Jiangsu Guoxin Investment Group Co., Ltd. (1.18 percent), Zhejiang Financial Development Company (2.64 percent) and Fujian Investment and Development Group Co., Ltd. (1.20 percent).

<sup>117</sup> The information displayed in the diagram is derived from *id.* at EB-32, EB-42, EB-67.

the denial of an international Section 214 authorization application where the applicant was indirectly owned and controlled by the Chinese government by finding that the applicant would be vulnerable to exploitation, influence and control by the Chinese government.<sup>118</sup> Like the applicant in *China Mobile*, China Telecom is indirectly majority-owned and controlled by the Chinese government and is vulnerable to exploitation, influence and control by the Chinese government.

First, China Telecom is wholly owned and controlled by a single Chinese entity—the Parent Entity.<sup>119</sup> [REDACTED]

[REDACTED] The Parent Entity is majority-owned and controlled by a state-owned enterprise under Chinese government supervision.<sup>121</sup> The Parent Entity has disclosed that the state-owned enterprise's controlling interests could result in actions that conflict with the interests of the Parent Entity or its shareholders.<sup>122</sup>

---

<sup>118</sup> *China Mobile Order*, 34 FCC Rcd. at 3368-71 ¶¶ 14-19; see also *id.* at 3368 ¶14 n.46 (citing Factors 3 and 4).

<sup>119</sup> Business Confidential Exhibit 3 at EB-13, *supra* note 73. [REDACTED]

<sup>120</sup> *Id.* at EB-13.

<sup>121</sup> Exhibit 4 at EB-42, *supra* note 83.

<sup>122</sup> *Id.* at EB-42 (“China Telecom Group, a state-owned enterprise . . . as our controlling shareholder, will continue to exercise significant influence over our management and policies. . . The interests of China Telecom Group as our controlling shareholder could conflict with our interests or the interests of our other shareholders. As a result, China Telecom Group may take actions with respect to our business that may not be in our or our other shareholders’ best

*Second*, China Telecom is ultimately majority-owned and controlled by the Chinese government. In *China Mobile*, the Commission was concerned about Chinese laws<sup>123</sup> and certain practices that the Chinese government could use to exploit, influence, and control a state-owned enterprise.<sup>124</sup> Some of the concerns raised by the Commission in *China Mobile* 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. For example, in *China Mobile*, the Commission noted a USTR 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."<sup>125</sup>

---

interests.").

<sup>123</sup> *China Mobile Order*, 34 FCC Rcd. at 3369 ¶ 17 ("Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world."); see also Exhibit 118 at EB-2735, China Law Translate, National Intelligence Law of the P.R.C. (2017), <https://www.chinalawtranslate.com/en/tag/national-intelligence-law/> (accessed May 29, 2019); see also Exhibit 120 at EB-2747, Murray Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July, 20, 2017), <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense> (citing laws on National Intelligence, Counterespionage, National Security, Counterterrorism, Cybersecurity, and Foreign NGO Management, amendments to PRC Criminal Law, Management Methods for Lawyers and Law Firms, and then-pending draft Encryption Law and draft Standardization Law); see also Exhibit 115 at EB-2524, Office of the Sec'y of Def. Ann. Rep. to Cong., *Military and Security Developments Involving the People's Republic of China 2019*, at 101 ("The 2017 *National Intelligence Law* requires Chinese companies, such as Huawei and ZTE, to support, provide assistance, and cooperate in China's national intelligence work, wherever they operate.").

<sup>124</sup> *China Mobile Order*, 34 FCC Rcd. at 3369-70 ¶ 18 (citing World Bank and USTR reports on Chinese state-owned enterprises demonstrating Chinese government exploitation, influence and control); see also Exhibit 116 at EB-2568, USTR, 2018 Report to Congress on China's WTO Compliance, at 13 (Feb. 2019).

<sup>125</sup> *China Mobile Order*, 34 FCC Rcd. at 3370 ¶ 18 n.60 (citing USTR 2018 Report to Congress on China's WTO Compliance); see also Exhibit 116 at EB-2568, *supra* note 124.

Such changes may have already occurred with respect to China Telecom. In January 2018, China Telecom's Parent Entity revised its Articles of Association to give the CCP greater powers,<sup>126</sup> three months after the Chinese government amended the Constitution of the CCP.<sup>127</sup> According to the Chinese government, the constitutional amendments were made to "define the status and role of Party organizations in State-owned enterprises."<sup>128</sup> State-owned enterprises would be required to form CCP organizations inside the enterprise to "focus their work on the operations of their enterprise," to "guarantee and oversee the implementation of the principles and policies of the Party and the state within their own enterprise," and "participate in making decisions on major issues in the enterprise."<sup>129</sup>

China Telecom's Parent Entity followed suit in January 2018 to revise Articles 9 and 98 of its Articles of Association to conform to the CCP constitutional amendments.<sup>130</sup> The Parent Entity's revised Articles of Association give CCP organizations within the company greater controls over the management and operations over the business. Article 9 of the revised Articles of Association states that:

---

<sup>126</sup> Exhibit 48 at EB-735 and EB-766, Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018 (Articles 9 and 98 of unofficial English translation of Articles of Association as filed with the SEC on Apr. 27, 2018 as part of Annual Report (Form 20-F)).

<sup>127</sup> Exhibit 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](http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf).

<sup>128</sup> Exhibit 113 at EB-2382, Full text of resolution on amendment to CPC Constitution, State Council of the People's Republic of China, [http://english.gov.cn/news/top\\_news/2017/10/24/content\\_281475919837140.htm](http://english.gov.cn/news/top_news/2017/10/24/content_281475919837140.htm) (Oct. 24, 2017).

<sup>129</sup> Exhibit 114 at EB-2404, *supra* note 127 (Article 33).

<sup>130</sup> Exhibit 48 at EB-735, 766, *supra* note 126 (Articles 9 and 98).

In 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.<sup>131</sup>

Article 98 of the Articles of Association states that:

Prior to making decisions on material issues of the Company, *the board of directors shall seek advice from the Party organisations.* When the board of directors appoints senior management personnel of the Company, the Party organisations shall consider and provide comments on the candidates for management positions nominated by the board of directors or the general manager, or recommend candidates to the board of directors and/or the general manager.<sup>132</sup>

The Parent Entity's prior Articles of Association did not mention the CCP.<sup>133</sup>

**C. Due to its ownership, China Telecom will be forced to comply with Chinese government requests without sufficient legal procedures subject to independent judicial oversight (Factors 6-7)**<sup>134</sup>

China Telecom will be forced to comply with Chinese government requests. It has already submitted to at least one foreign request from its Parent Entity without sufficient legal process or judicial oversight. As discussed above in Section IV.A.1, *supra*, China Telecom has already complied [REDACTED]


---

<sup>131</sup> *Id.* at EB-735 (emphasis added).

<sup>132</sup> *Id.* (emphasis added).

<sup>133</sup> Compare Exhibit 49 at EB-798, China Telecom Corp. Ltd., Annual Report (Form 20-F) (Apr. 28, 2016), Ex. 1.1 (Articles of Association of China Telecom Corp. Ltd. as of May 27, 2015) with Exhibit 48 at EB-732, *supra* note 126, at Ex. 1.1 (Articles of Association of China Telecom Corp. Ltd. as of Jan. 4, 2018).

<sup>134</sup> Factor 6 considers whether a carrier will be required to comply with foreign requests due to its foreign ownership. Factor 7 considers whether any foreign requests to the carrier would be governed by publicly available legal procedures subject to independent judicial oversight.



The Chinese government's controls over the Parent Entity and China Telecom, combined with newly enacted Chinese laws, raise significant concerns that China Telecom will be forced to comply with Chinese government requests, including requests for communications intercepts, without the ability to challenge such requests. These new laws include the Cybersecurity Law of the People's Republic of China, effective June 1, 2017, and the implementing regulation for the Cybersecurity Law, effective November 1, 2018.

The June 1, 2017 Cybersecurity Law requires extensive cooperation by telecom and

---

<sup>135</sup> Business Confidential Exhibit 36 at EB-621, *supra* note 63.

<sup>136</sup> *Id.* at EB-629, attachment B: U.S. Records Security Agreement, at 9 ¶ 6.2.



network operators:

Article 35: Critical 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.

...

Article 49: Network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law.<sup>137</sup>

According to the Parent Entity's interpretation of the 2017 Cybersecurity Law, the law sets forth a "cybersecurity review" that government authorities could initiate that would focus on the "controllability" of network products and services.<sup>138</sup>

The November 1, 2018 "Regulation on Internet Security Supervision by Public Security Organs" (Order No. 151 of the Ministry of Public Security) provided further directives for implementing the 2017 Cybersecurity Law.<sup>139</sup> The 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.<sup>140</sup> The People's Armed Police would also be present at inspections to

---


<sup>137</sup> Exhibit 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/>.

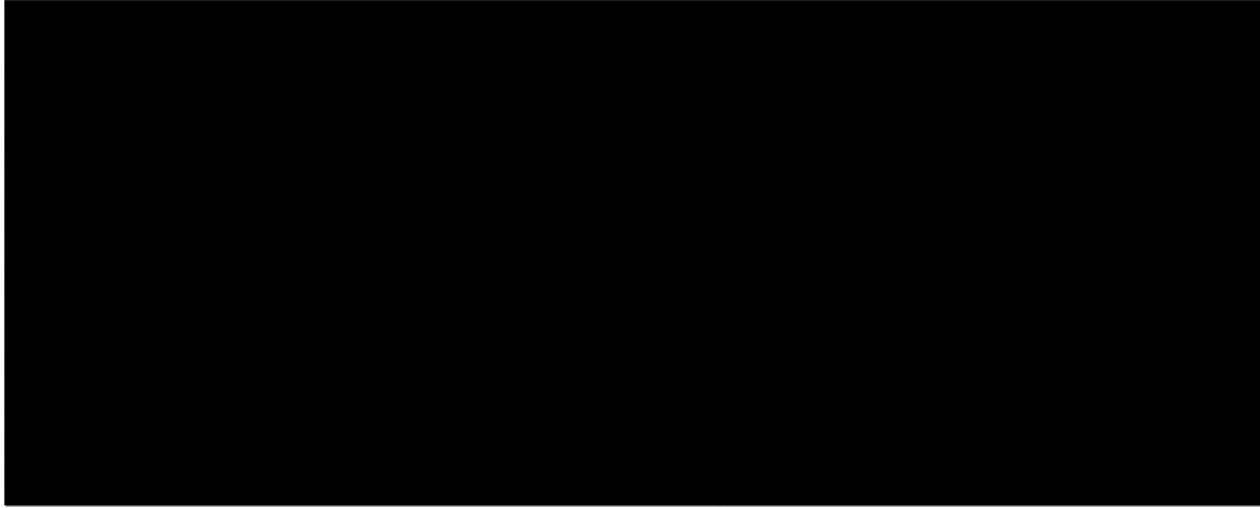
<sup>138</sup> Exhibit 4 at EB-86, *supra* note 83.

<sup>139</sup> See Exhibit 53 at EB-901, *China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers Issued*, Library of Congress (Nov. 13, 2018), <http://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-inspection-powers-issued/>; see also Exhibit 54 at EB-903, *China's New Cybersecurity Measures Allow State Policy to Remotely Access Company Systems*, Recorded Future Blog (Feb. 8, 2019), <https://www.recordedfuture.com/china-cybersecurity-measures/>.

<sup>140</sup> Exhibit 54 at EB-904, *supra* note 139.

ensure compliance with the inspection.<sup>141</sup> For remote inspections, the Ministry of Public Security would be permitted to use certain cybersecurity service agencies.<sup>142</sup>

Both the 2017 Cybersecurity Law and 2018 Regulation on Internet Security Supervision provide little, if any, detail about the available legal procedures or judicial oversight to challenge any Chinese government requests. According to industry sources, these new laws codified existing practices rather than imposing wholly new obligations.<sup>143</sup> The 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 has disclosed that, 



---

<sup>141</sup> *Id.* at EB-907, EB-909.

<sup>142</sup> *Id.* at EB-905.

<sup>143</sup> Exhibit 56 at EB-921, Covington & Burling LLP., *China Releases New Regulation on Cybersecurity Inspection*, Inside Privacy (Oct. 23, 2018), <https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/>.

<sup>144</sup> Exhibit 36 at EB-634, *supra* note 63.

**D. China Telecom's U.S. operations provide opportunities for Chinese state-sponsored actors to engage in economic espionage and to disrupt and misroute U.S. communications traffic (Factors 5, 8-12)<sup>145</sup>**

China Telecom's 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. As explained in Section II, *supra*, 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.<sup>146</sup>

1. China Telecom's U.S. operations provide opportunities for Chinese government-sponsored actors to engage in economic espionage against U.S. targets (Factors 5, 9-12)

China Telecom's U.S. operations provide the Chinese government with access to valuable targets for economic espionage and other intellectual property and privacy-related thefts. The international Section 214 authorizations furnish China Telecom with access to more customers, communications traffic, and interconnections with other U.S. common carriers than it

---

<sup>145</sup> Factor 5 considers whether a carrier's foreign ownership is from a country suspected of engaging in actions, or possessing the intention to take actions, that could impair national security. Factor 8 considers whether a carrier's U.S. operations provide opportunities for actors to undermine the reliability of domestic communications infrastructure. Factor 9 considers whether a carrier's U.S. operations provide opportunities for actors to expose national security vulnerabilities. Factor 10 considers whether a carrier's U.S. operations provide opportunities to render communications infrastructure vulnerable to exploitation or covert monitoring. Factor 11 considers whether a carrier's U.S. operations provide opportunities for foreign actors to engage in economic espionage against U.S. corporations. Factor 12 considers whether a carrier's U.S. operations provide opportunities for actors to engage in other activities with potential national security implications.

<sup>146</sup> Exhibit 8 at EB-351, *supra* note 4.

would have otherwise. Moreover, China Telecom intentionally markets its services as secure to customers in industries highly vulnerable to economic espionage, such as the financial, logistics, retail, media, energy, and healthcare industries.<sup>147</sup>

China Telecom's status as a managed services provider (MSP) provides abundant opportunities for Chinese government-sponsored actors, as described in a recent federal indictment. According to the December 2018 *Zhu* indictment, Chinese hackers working in association with the Chinese Ministry of State Security targeted MSPs in order to "leverage the MSPs' networks to gain unauthorized access to the computers and computer networks of the MSPs' clients and steal, among other data, intellectual property and confidential business data on a global scale."<sup>148</sup> If data centers and corporate intranets are the information economy's equivalent to banks, then an MSP's access to its clients' networks and data centers puts potential bank robbers one step closer to circumventing a bank's security apparatus.

China Telecom's managed network and security services similarly provide opportunities for Chinese government-sponsored cyber actors. According to the October 2018 *Zhang* indictment, in one cyber intrusion of a French company, a Chinese intelligence officer reported to a colleague that "[w]e sent a fake email pretending to be from network management."<sup>149</sup> Through China Telecom, Chinese government-sponsored cyber actors may have access to China Telecom's network management and security services. They also have access to the Parent Entity, which is now required by its Articles of Association to carry out functions for and seek the advice of the CCP. Next time, Chinese government-sponsored cyber actors may no longer

---

<sup>147</sup> Exhibit 42 at EB-699, *supra* note 97.

<sup>148</sup> Exhibit 100 at EB-2074, *supra* note 15.

<sup>149</sup> Exhibit 98 at EB-2034, *supra* note 13.

need to pretend to be from network management—they might actually be from network management.

China Telecom's access to its clients' U.S. records may provide additional opportunities for Chinese government-sponsored cyber actors. China Telecom's largest U.S. customers include [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] As previously mentioned, China Telecom [REDACTED]

[REDACTED]

[REDACTED]

Concerns about such access are heightened by prior reporting that China Telecom's Chinese affiliates have aided the Chinese government's economic espionage efforts. According to Mandiant (now FireEye), China Telecom's Parent Entity has provided special fiber optic communications infrastructure to house a known state-sponsored military cyber unit.<sup>153</sup>

Mandiant has alleged that this Chinese military unit has stolen hundreds of terabytes of sensitive data from at least 141 organizations across a diverse set of organizations.<sup>154</sup>

---

<sup>150</sup> Business Confidential Exhibit 107 at EB-2148, Letter from Morgan Lewis to DOJ National Security Division, Exhibit B (April 18, 2019).

<sup>151</sup> Business Confidential Exhibit 36 at EB-634, *supra* note 63, at Exhibit B.

<sup>152</sup> Business Confidential Exhibit 103 at EB-2113, *supra* note 67.

<sup>153</sup> Exhibit 70 at EB-1468, EB-1471, Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> (Feb. 19, 2013).

<sup>154</sup> *Id.* at EB-1455.

2. China Telecom's operations in the United States provide opportunities for Chinese government-sponsored actors to disrupt and misroute U.S. communications traffic (Factors 8-10, 12)

Factors 8-10 and 12, when evaluated in light of reports that China Telecom has disrupted and misrouted Internet traffic (including U.S. government Internet traffic), also weigh in favor of revocation and termination.

China Telecom's U.S. operations, particularly its eighteen (18) Points of Presence (PoPs) in the United States,<sup>155</sup> provide Chinese government-sponsored actors with openings to disrupt and misroute U.S. data and communications traffic. In November 2018, industry monitors observed that Google services were made unavailable to U.S. enterprise users for over an hour, because China Telecom's network announced erroneous route information.<sup>156</sup> In late 2018 and early 2019, during the partial U.S. government shutdown, private security watchers detected China Telecom's network misrouting the U.S. Department of Energy's Internet traffic.<sup>157</sup>

The misrouting incidents are not isolated incidents but part of a pattern going back to 2010.<sup>158</sup> These incidents are believed to result from Border Gateway Protocol (BGP)<sup>159</sup>

---

<sup>155</sup> Exhibit 6 at EB-296, *supra* note 37; see also <https://www.ctamericas.com/global-data-center-map/> (last visited Feb. 1, 2019).

<sup>156</sup> See Exhibit 71 at EB-1527, Ameet Naik, *Internet Vulnerability Takes Down Google*, Thousand Eyes Blog (Nov. 12, 2018), <https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/>; see also Exhibit 72 at EB-1535, Press Release, China Telecom Corp. Ltd., Statement Regarding the Unfounded Report on China Telecom Being Alleged "Hijacking Internet Traffic," <http://www.irasia.com/listco/hk/chinatelecom/press/p181122.htm> (last visited Jan. 23, 2019).

<sup>157</sup> See Exhibit 87 at EB-1948, China Telecom hijack of US Dept. of Energy route continuing into 6th day (Jan. 2, 2019), <https://twitter.com/internetintel/status/1080466509292621829>; see also Exhibit 88 at EB-1951, *Possible BGP hijack*, BGPMon (Dec. 28, 2018), <https://bgpstream.com/event/171779>.

<sup>158</sup> See Exhibit 73 at EB-1786-87, 2010 Rep. to Congress of the U.S.-China Econ. & Security Rev. Commission, at 243-44 (November 2010); Exhibit 74 at EB-1860, *Chinese ISP hijacks the Internet*, BGPMon (Apr. 8, 2010), <https://bgpmon.net/chinese-isp-hijacked-10-of-the->

announcement errors, in which China Telecom either originated erroneous route information, or propagated and amplified erroneous route information by advertising it to U.S. peering partners. BGP assumes the truthful and correct advertising of BGP routes on the Internet and, accordingly, is subject to abuse by unscrupulous (or incompetent) actors.

Isolated incidents of misrouting, if quickly identified and corrected, may have limited impact. But that is not the case for China Telecom. For nearly a decade, China Telecom has been on notice that its network advertised incorrect routing information to its neighbors on the Internet. Public reports have claimed that China Telecom's network<sup>160</sup> misrouted large amounts of information and communications traffic, over long periods of time (often several months), sometimes involving U.S. government traffic. For example:

- **April 8, 2010 (15 percent of available routes worldwide):** For about 18 minutes, China Telecom advertised erroneous network traffic routes that instructed U.S. and other foreign Internet traffic to travel through Chinese servers. Other servers around the world quickly adopted these paths, incorrectly advertising about 15 percent of all available

---

internet/; Exhibit 75 at EB-1866, Demchak, C. and Shavitt, Y, China's Maxim – Leave No Access Point Unexploited: the Hidden Story of China Telecom's BGP Hijacking, Military Cyber Affairs, Vol. 3: Iss. 1, Article 7 (2018).

<sup>159</sup> BGP is the routing method that enables the Internet to route information and is a vital part of the Internet infrastructure. Much like a GPS navigation system, the BGP routing protocol provides directions for individual packets of data traveling across independently operated networks on the Internet. BGP uses an Autonomous System (AS) architecture, under which each autonomous system (such as a network operated by a university or Internet Service Provider) is assigned a unique Autonomous System Number (ASN). Under BGP, these ASNs collect routing information from their neighboring ASNs (peers) about what routes are available at that moment, and then propagate that routing information further, which results in creating dynamically updated information about available routes on the Internet. The BGP protocol is used to determine which of the available routes is most suitable.

<sup>160</sup> References to "China Telecom's network" here refer to both China Telecom's network as well as its Parent Entity's network, which is consistent with China Telecom's own usage. See Exhibit 81 at EB-1899, China Telecom Americas – Global Network, <https://www.ctamericas.com/company/global-network> (accessed Mar. 11, 2019) (interchangeably referring to its own network and its Parent Entity's network, ChinaNet AS4134, as one "Global Network").

routes on the Internet to transit through China.<sup>161</sup>

- **March 2011 (Facebook U.S. traffic):** Traffic to Facebook.com from AT&T was routed through China Telecom.<sup>162</sup>
- **December 2015 through 2017 (Verizon traffic):** China Telecom advertised erroneous routing information such that Verizon traffic was routed through China for many months through 2017.<sup>163</sup>
- **February to August 2016 (Canada & South Korea government traffic):** China Telecom erroneously advertised routes such that traffic between Canadian and South Korean government sites were routed through China Telecom's PoP in Los Angeles and forwarded to China.<sup>164</sup>
- **October 2016 (U.S. & Italy bank traffic):** China Telecom erroneously advertised routes such that traffic from the United States to a large Anglo-American bank headquartered in Milan, Italy, was routed through China Telecom's PoP in Los Angeles and forwarded to China.<sup>165</sup>
- **April to May 2017 (Sweden/Norway to Japan involving U.S. media traffic):** China Telecom also erroneously advertised routes such that traffic between Sweden, Norway and Japan, involving a large U.S. news organization, was routed through China Telecom's PoP in California and forwarded to China before being sent to Japan.<sup>166</sup>
- **April to July 2017 (Italy to Thailand traffic, affecting U.S. ISPs Cogent and Level 3):** China Telecom also erroneously advertised routes from its Los Angeles PoP such that traffic from Italy to Thailand was routed through China. The erroneous route information affected large U.S. Internet service providers, including Cogent and Level 3, as well as South Korean providers.<sup>167</sup>

---

<sup>161</sup> Exhibit 73 at EB-1786-77, *supra* note 158.

<sup>162</sup> Exhibit 76 at EB-1877, Andree Toonk, *Facebook's detour through China and Korea*, BGPMon (Mar. 26, 2011), <https://bgpmon.net/facebooks-detour-through-china-and-korea/>.

<sup>163</sup> Exhibit 77 at EB-1880, Doug Madory, *China Telecom's Internet Traffic Misdirection*, VantagePoint Blog (Nov. 5, 2018), <https://dyn.com/blog/china-telecoms-internet-traffic-misdirection/>; Exhibit 75 at EB-1872-73, *supra* note 158.

<sup>164</sup> Exhibit 75 at EB-1872-73, *supra* note 158.

<sup>165</sup> *Id.* at EB-1873.

<sup>166</sup> *Id.* at EB-1874.

<sup>167</sup> *Id.* at EB-1874.



- **November 13, 2018 (Google worldwide traffic, including G Suite, Google Search and Google Analytics):** For over an hour, China Telecom also erroneously advertised routes from a Nigerian ISP that resulted in traffic being routed through China and terminating at a China Telecom edge router.<sup>168</sup>
- **December 2018-January 2019 (U.S. Department of Energy traffic):** Private security watchers detected the re-routing of U.S. Department of Energy Internet traffic associated with erroneous route information announced by China Telecom's network.<sup>169</sup>
- **June 6, 2019 (European mobile provider traffic, including U.S.-Europe traffic):** For more than two hours, traffic destined for Europe's largest mobile providers was routed through China Telecom's network, resulting in significant outages that affected WhatsApp availability in the United States.<sup>170</sup> This most recent event occurred months after Team Telecom specifically asked China Telecom [REDACTED]

When asked to explain, China Telecom claimed that [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>168</sup> Exhibit 71 at EB-1527, *supra* note 156; Exhibit 72 at EB-1535, *supra* note 156 (Parent Entity acknowledging that China Telecom forwarded "erroneous routing configuration by a Nigerian operator" thus "resulting in severe congestion").

<sup>169</sup> Exhibit 88 at EB-1951, *supra* note 157.

<sup>170</sup> Exhibit 121 at EB-2751, Doug Madory, *Large European Routing Leak Sends Traffic Through China Telecom*, Oracle Blog (June 6, 2019), <https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom>; *see also* Exhibit 122 at EB-2761, Archana Kesavan, *WhatsApp Disruption: Just One Symptom of Broader Route Leak*, ThousandEyes Blog (June 7, 2019), <https://blog.thousandeyes.com/whatsapp-disruption-just-one-symptom-of-broader-route-leak/>; Exhibit 123 at EB-2768, Dan Goodin, *BGP event sends European mobile traffic through China Telecom for 2 hours*, Ars Technica (June 8, 2019), <https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/>.

<sup>171</sup> *See* Business Confidential Exhibit 78 at EB-1890, Attachment to E-mail from Morgan Lewis to DOJ National Security Division (Jan 23, 2019) (providing responses to questions regarding press reports of China Telecom's alleged BGP hijacking).

<sup>172</sup> *Id.* at EB-1892.

[REDACTED]

[REDACTED] Unlike other large data and communications providers in the United States (such as Charter, Cogent, Comcast, CenturyLink, Google, and Microsoft), China Telecom did not join the Internet Society's Mutually Agreed Norms for Routing Security or other efforts to improve routing security.<sup>177</sup> China Telecom has instead argued that [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>173</sup> *Id.* at EB-1892 (response to Question No. 10).

<sup>174</sup> *Id.* at EB-1893 (response to Question No. 11).

<sup>175</sup> *Id.* at EB-1893 (response to Question No. 10).

<sup>176</sup> *Id.* at EB-1893 (response to Question No. 10).

<sup>177</sup> Exhibit 111 at EB-2189, Network Operator Participants, Mutually Agreed Norms for Routing Security, <https://www.manrs.org/isps/participants/> (last visited May 1, 2019); *see also* Exhibit 121 at EB-2759, *supra* note 170 (Oracle security analyst stating that a "great place for any telecom to start improving their routing hygiene is to join the Internet Society's Mutually Agreed Norms for Routing Security (MANRS) project.").

<sup>178</sup> Business Confidential Exhibit 78 at EB-1890, *supra* note 171 (response to Question No. 1).

[REDACTED] This argument is akin to a hazardous chemicals manufacturer arguing that the public need not worry about its failure to monitor safety conditions or follow voluntary fire safety codes, because nothing has exploded yet, and even if it did, it would not be purposeful.

In today's national security environment, China Telecom's access to the U.S. communications network, [REDACTED] [REDACTED] creates a vulnerability that is just as real as failing to monitor flammable fumes on a factory floor. China Telecom's U.S. operations present opportunities, and plausible deniability, for Chinese state-sponsored actors to disrupt and misroute U.S. Internet traffic. China Telecom today operates [REDACTED] [REDACTED] and has 18 PoPs where it accesses the U.S. communications network at all major U.S. interconnection points, including those located in Ashburn, Virginia; Los Angeles, California; New York City; Silicon Valley (San Jose, Santa Clara and Palo Alto, California).<sup>180</sup> China Telecom also advertises BGP routing information to peering partners, including [REDACTED] [REDACTED] [REDACTED]

China Telecom's presence in the United States worsened the effects of the November 13, 2018 incident in which its erroneous BGP route advertisements interrupted Google services for

---

<sup>179</sup> *Id.* at EB-1891 (response to Question No. 3).

<sup>180</sup> Exhibit 6 at EB-296, *supra* note 37.

<sup>181</sup> Business Confidential Exhibit 78 at EB-1891, *supra* note 171 (response to Question No. 6); Exhibit 79 at EB-1894, *China Telecom*, PeeringDB, <https://www.peeringdb.com/net/308> (last visited Feb. 8, 2019).

more than an hour. China Telecom's Parent Entity admitted that it forwarded erroneous routes received from its Nigerian peer.<sup>182</sup> This erroneous information was then disseminated to China Telecom's peering partners (including those in the United States).<sup>183</sup> In a vacuum, a Nigerian network advertising erroneous BGP routes may have limited impact on the United States. But China Telecom's extensive U.S. presence amplified that error when China Telecom forwarded that misinformation to U.S. peers and caused U.S. traffic to detour through China. Once that traffic went to China, it terminated at a China Telecom edge router, causing a massive denial of service to Google's services.<sup>184</sup> Industry observers noted that, despite past reports, China Telecom "still" has not "reined in their infrastructure for any type of filtering," showing "how inherently fragile BGP is being based on trust. Also [ ] this isn't new."<sup>185</sup> China Telecom's

[REDACTED]

[REDACTED] is unreasonable given its public history of BGP incidents.

China Telecom's U.S. presence also allows China to disrupt U.S. Internet traffic for political purposes. ODNI warned this year that China is "capable of using cyber attacks against systems in the United States to censor or suppress viewpoints it deems politically sensitive."<sup>186</sup> One example is China Telecom's seeming involvement in the "Great Cannon" denial of service

---

<sup>182</sup> Exhibit 72 at EB-1535, *supra* note 156.

<sup>183</sup> Exhibit 71 at EB-1530, *supra* note 156.

<sup>184</sup> *See id.*

<sup>185</sup> Exhibit 101 at EB-2099, Dan Goodin, *Google goes down after major BGP mishap routes traffic through China*, Ars Technica (Nov. 13, 2018), <https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/>.

<sup>186</sup> Exhibit 8 at EB-353, *supra* note 4.

attacks.<sup>187</sup> According to an April 2015 paper published by the University of Toronto's Citizen Lab, China Telecom's network was used to insert malicious code onto computers in the United States visiting Chinese sites.<sup>188</sup> The computers were then reportedly co-opted to carry out the "Great Cannon" distributed denial of service attack on GitHub and GreatFire.org.<sup>189</sup> The 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.<sup>190</sup>

**E. China Telecom's lack of trustworthiness limits the Executive Branch's ability to conduct statutorily authorized law enforcement and national security missions, and to protect information about targets and classified sources and missions (Factors 13, 14)<sup>191</sup>**

The Executive Branch agencies believe that China Telecom's 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. The U.S.

---

<sup>187</sup> Exhibit 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>.

<sup>188</sup> *Id.*

<sup>189</sup> *Id.*; see also Exhibit 105 at EB-2134, James Griffiths, *When Chinese hackers declared war on the rest of us*, MIT Technology Review (Jan. 10, 2019), <https://www.technologyreview.com/s/612638/when-chinese-hackers-declared-war-on-the-rest-of-us/>.

<sup>190</sup> Exhibit 104 at EB-2123, *supra* note 187; Exhibit 105 at EB-2135, *supra* note 189.

<sup>191</sup> Factor 13 considers whether the Executive Branch will be able to continue to conduct its statutorily authorized law enforcement and national security missions, which may include issuance of legal process for the production of information or provision of technical assistance. Factor 14 considers whether the confidentiality requirements that protect information about the targets of lawful surveillance and classified sources and methods will continue to be effective.

government would not be able to work effectively with China Telecom 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. These carriers must be willing to share accurate information with the U.S. government and to cooperate fully in investigations. The government must be able to trust that the information it provides to carriers will be kept in confidence and used by the carrier solely for the purpose of protecting its networks.

In certain instances, however, China Telecom's indirect ownership and control by the Chinese government may result in particular sensitivities that could impair China Telecom's compliance with lawful U.S. process that seeks information transmitted using networks connected to China. In other instances, U.S. authorities may have particular sensitivities that could limit sharing of information with China Telecom due to concerns that its Parent Entity and other Chinese affiliates would become aware of U.S. authorities' investigative interests in information related to China Telecom's services. Because China Telecom is ultimately owned by the Chinese government, the U.S. government cannot trust China Telecom to identify, disrupt, or provide assistance for investigations into unlawful activity sponsored by the Chinese government.

Given these facts, the Executive Branch, through Team Telecom, cannot rely on China Telecom's assistance to conduct statutorily authorized law enforcement and national security missions, such as serving legal process or receiving technical assistance in the prosecution thereof, and cannot trust that China Telecom will protect information about classified or otherwise sensitive sources and missions.

**V. The Executive Branch does not recommend further mitigation**

The Executive Branch does 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.<sup>192</sup> China Telecom 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:

- (1) To make U.S. records available in the United States in response to lawful U.S. process;
- (2) To take all practicable measures to prevent unauthorized access to U.S. records;
- (3) Not to disclose or permit access to U.S. records or U.S. law enforcement demands in response to foreign government request, unless certain safeguards are met, and to notify U.S. authorities promptly if foreign government requests are received;
- (4) To maintain a U.S. point of contact for accepting and overseeing compliance with U.S. law enforcement demands made pursuant to lawful process; and
- (5) To notify DOJ, FBI, and DHS of material changes to China Telecom's services, or of any action requiring notice or application to the FCC.<sup>193</sup>

China Telecom has breached at least two of the five LOA provisions, including provisions (2) and (5). As stated in the LOA, breaching any of these conditions provides independent grounds

---

<sup>192</sup> See *China Mobile Order*, 34 FCC Rcd. at 3380 ¶ 38 (“[W]e acknowledge the Executive Branch’s established role in monitoring and enforcing compliance with mitigation agreements and, therefore, we conclude that it is appropriate to defer to what we believe to be a reasonable assertion of the Executive Branch agencies that mitigation is not an adequate option here.”).

<sup>193</sup> Exhibit 1 at EB-1-3, *supra* note 23.

for revoking or terminating China Telecom's Section 214 authorizations.<sup>194</sup>

*First*, China Telecom, as required by the LOA, failed to take "all practicable measures" to prevent unauthorized access to U.S. records. [REDACTED]

[REDACTED]

---

<sup>194</sup> *Id.* at EB-3 ("The Company agrees that, in the event the commitments set forth in this [LOA] are breached, . . . the DOJ, FBI, or DHS may request that the FCC . . . revoke, [or] cancel . . . any relevant license, permit or other authorization granted by the FCC to the Company").

<sup>195</sup> Business Confidential Exhibit 119 at EB-2745, *supra* note 72; *see also* Business Confidential Exhibit 124 at EB-2775-76, *supra* note 93.

<sup>196</sup> *Compare* Business Confidential Exhibit 103 at EB-2113, *supra* note 67 [REDACTED]  
[REDACTED] *with* Business Confidential Exhibit 36 at EB-624, *supra* note 63  
[REDACTED]

<sup>197</sup> Business Confidential Exhibit 102 at EB-2103, *supra* note 89; *see also* Business Confidential Exhibit 109 at EB-2170, Letter from Morgan Lewis to DOJ National Security Division (Mar. 27, 2019); Business Confidential Exhibit 103 at EB-2107, *supra* note 67; Business Confidential Exhibit 119 at EB-2745, *supra* note 72; Business Confidential Exhibit 124 at EB-2774, *supra* note 93.



[REDACTED]

*Second*, China Telecom failed to inform the FBI, DOJ and DHS at least twice in 2010 when it filed notices to the FCC.<sup>199</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

China Telecom's 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 should not be trusted to comply with more stringent mitigation measures. Even if China Telecom had proposed mitigation measures, they would likely be insufficient to address newly discovered risks in today's rapidly evolving threat environment.

China Telecom has also demonstrated an unwillingness to cooperate with mitigation monitoring. Despite 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

---

<sup>198</sup> Business Confidential Exhibit 103 at EB-2107, *supra* note 67; Business Confidential Exhibit 119 at EB-2745, *supra* note 72.

<sup>199</sup> Business Confidential Exhibit 103 at EB-2108-2109, *supra* note 67 (citing FCC file numbers SPC-NEW-20100326-00007 and SPC-NEW-20100314-00006).

<sup>200</sup> *Id.* at EB-2108; Business Confidential Exhibit 119 at EB-2745-2746, *supra* note 72; Business Confidential Exhibit 124 at EB-2774, *supra* note 93.

U.S. government cannot rely on China Telecom to do so. In response to a Team Telecom request for cybersecurity policies, China Telecom delayed for six months before it provided an improperly redacted document. When the redaction was finally removed, China Telecom's underlying motivation could not have been more clear: China Telecom wished [REDACTED]

[REDACTED]

Because China Telecom failed to comply with its LOA and has signaled its unwillingness to enter into a more effective agreement, the Executive Branch does not recommend further mitigation.

## **VI. Conclusion**

The Executive Branch recommends revocation and termination of China Telecom's existing international Section 214 authorizations to operate as an international common carrier. The present or future public convenience and necessity do not require China Telecom's international common carrier services in the current national security environment. Instead, China Telecom's operations in the United States now pose substantial and unacceptable risks to U.S. national security and law enforcement concerns.

---

<sup>201</sup> Business Confidential Exhibit 37 at EB-655, *supra* note 65 (emphasis added).

**[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]**

Although the information set forth above is independently sufficient to justify recommendation of revocation and termination, the Executive Branch has also provided additional relevant information in the classified annex.

Respectfully submitted:



Kathy D. Smith  
Chief Counsel

National Telecommunications and Information  
Administration

U.S. Department of Commerce Rm 4713  
14th Street and Constitution Ave., N.W.  
Washington, D.C. 20230  
(202) 482-1816

April 9, 2020

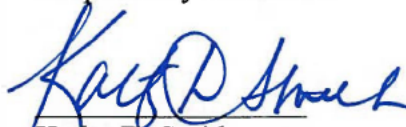
**CERTIFICATE OF SERVICE**

I, Kathy Smith, hereby certify that consistent with 47 C.F.R. § 1.47 I have served a copy of the foregoing by certified mail this 9<sup>th</sup> day of April, 2020 to the following:

Andrew Lipman  
Catherine Wang  
Ulises Pin  
Morgan Lewis  
1111 Pennsylvania Ave, NW  
Washington, DC 20004  
andrew.lipman@morganlewis.com  
catherine.wang@morganlewis.com  
ulises.pin@morganlewis.com  
COUNSEL FOR CHINA TELECOM (AMERICAS) CORP.

Luis Fiallo  
Vice President  
China Telecom (Americas) Corp.  
607 Herndon Parkway, No. 201  
Herndon, VA 20170  
(703) 787-0088 ext. 18  
(703) 787-0086  
lfiallo@ctamericas.com

Respectfully submitted:

  
Kathy D. Smith  
Chief Counsel

**Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, D.C. 20554**

In the Matter of	)	
	)	
<b>CHINA TELECOM (AMERICAS) CORPORATION</b>	)	File Nos.
	)	
<b>f/k/a CHINA TELECOM (USA) CORPORATION</b>	)	ITC-214-20010613-00346;
	)	ITC-214-20020716-00371;
	)	ITC-T/C-20070725-00285.
	)	

**Executive Branch Recommendation to the Federal Communications Commission to  
Revoke and Terminate China Telecom’s International Section 214 Common Carrier**

**Authorizations**

**INDEX OF EXHIBITS**

<b>Ex. No.</b>	<b>Business Confidential</b>	<b>Description</b>	<b>Start Page</b>
1.		July 17, 2007 Letter of Assurance from Yi-jun Tan to DOJ, FBI and DHS	EB-1
2.		China Telecom (USA) Corporation Stock Purchase Agreement (June 15, 2007)	EB-4
3.	X	Responses of China Telecom (USA) Corporation to Combined Questions for FCC Applicants (May 11, 2007)	EB-11
4.		China Telecom Corp. Ltd., Annual Report Form 20-F (Apr. 27, 2018)	EB-26
5.		China Telecom Americas, Solutions, <a href="https://www.ctamericas.com">https://www.ctamericas.com</a> (accessed Feb. 4, 2019)	EB-295
6.		Compiled list of China Telecom’s U.S. PoPs (Points of Presence), Colocation facilities and Cloud Exchanges and screenshots of Global Data Center Map, <a href="https://www.ctamericas.com/global-data-center-map/">https://www.ctamericas.com/global-data-center-map/</a> (accessed Feb. 1, 2019)	EB-296
7.		Unclassified Statement for the Record, Annual Threat Assessment, Senate Select Committee on Intelligence, Director of National Intelligence John D. Negroponte (Jan. 11, 2007)	EB-332

[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

Ex. No.	Business Confidential	Description	Start Page
8.		Statement for the record, Worldwide Threat Assessment of the U.S. Intelligence Community, Senate Select Committee on Intelligence, Director of National Intelligence Daniel R. Coats (Jan. 29, 2019).	EB-347
9.		General FAQs – China Telecom Americas, <a href="https://www.ctamericas.com/faqs">https://www.ctamericas.com/faqs</a> (accessed Feb. 26, 2019)	EB-389
10.		<i>International Authorizations Granted</i> , Public Notice, Report No. TEL-01179, DA No. 07-3632 at 3 (Aug. 16, 2007)	EB-393
11.		<i>International Authorizations Granted</i> , Public Notice, Report No. TEL-00567, DA No. 02-2060 (Aug. 22, 2002)	EB-398
12.		<i>International Authorizations Granted</i> , Public Notice, Report No. TEL-00423, DA No. 01-1794 (July 26, 2001)	EB-407
13.		Federal Reserve Foreign Exchange Rates, RMB to USD, <a href="https://www.federalreserve.gov/releases/h10/hist/dat00)ch.htm">https://www.federalreserve.gov/releases/h10/hist/dat00)ch.htm</a> (accessed Feb. 26, 2019)	EB-412
14.		Screenshot, Global Data Center Map, <a href="https://www.ctamericas.com/global-data-center-map">https://www.ctamericas.com/global-data-center-map</a> (accessed Feb. 26, 2019)	EB-522
15.-		<i>Intentionally blank</i>	<i>EB-523 to EB-525</i>
16.		International Private Leased Circuit from China Telecom Americas, China Telecom Americas, <a href="https://www.ctamericas.com/wp-content/uploads/2018/10/IPLC.pdf">https://www.ctamericas.com/wp-content/uploads/2018/10/IPLC.pdf</a> (accessed Feb. 12, 2019)	EB-526
17.		International Ethernet Private Line from China Telecom Americas, China Telecom Americas, <a href="https://www.ctamericas.com/wp-content/uploads/2018/10/IEPL.pdf">https://www.ctamericas.com/wp-content/uploads/2018/10/IEPL.pdf</a> (accessed Feb. 12, 2019)	EB-528
18.		International Private Lines, China Telecom, <a href="https://www.ctamericas.com/products-services/data-networking/international-private-lines/">https://www.ctamericas.com/products-services/data-networking/international-private-lines/</a> (accessed Mar. 4, 2019)	EB-530
19.		China Telecom Virtual Private LAN service, <a href="https://www.ctamericas.com/wp-content/uploads/2018/10/VPLS-Brochure.pdf">https://www.ctamericas.com/wp-content/uploads/2018/10/VPLS-Brochure.pdf</a> (accessed Feb. 26, 2019)	EB-533

**[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]**

20.		China Telecom Americas – MPLS VPN, <a href="https://www.ctamericas.com/products-services/data-networking/mpls-vpn/">https://www.ctamericas.com/products-services/data-networking/mpls-vpn/</a> (accessed Feb. 26, 2019)	EB-535
21.		China Telecom Americas – Software Defined WAN, <a href="https://www.ctamericas.com/products-services/data-networking/software-defined-wan/">https://www.ctamericas.com/products-services/data-networking/software-defined-wan/</a> (last visited Feb. 26, 2019)	EB-539
22.		China Telecom Americas, CTEExcel, <a href="https://www.ctexcel.us/index_pc.jsp?language=en">https://www.ctexcel.us/index_pc.jsp?language=en</a> (accessed Feb. 26, 2019)	EB-542
23.		Press Release, China Telecom has big US plan, <a href="https://www.ctamericas.com/china-telecom-big-us-plan/">https://www.ctamericas.com/china-telecom-big-us-plan/</a> (Jan. 15, 2016).	EB-546
24.		How is CTEExcel’s mobile plan the best for international students, Quora.com, <a href="https://www.quora.com/How-is-CTExcels-mobile-plan-the-best-for-international-students-Has-anyone-used-it-before">https://www.quora.com/How-is-CTExcels-mobile-plan-the-best-for-international-students-Has-anyone-used-it-before</a> (accessed Feb. 13, 2019)	EB-549
25.		Managed WAN – China Telecom Americas, <a href="https://www.ctamericas.com/products-services/managed-services/managed-wan/">https://www.ctamericas.com/products-services/managed-services/managed-wan/</a> (accessed Feb. 28, 2019)	EB-553
26.		China Telecom Americas, ICT Services, <a href="https://www.ctamericas.com/wp-content/uploads/2018/10/ICT-Services.pdf">https://www.ctamericas.com/wp-content/uploads/2018/10/ICT-Services.pdf</a> (accessed Feb. 12, 2019)	EB-556
27.		Public Cloud Exchange, China Telecom Americas, <a href="https://www.ctamericas.com/public-cloud-exchange/">https://www.ctamericas.com/public-cloud-exchange/</a> (accessed Mar. 1, 2019)	EB-558
28.		Colocation Services, China Telecom Americas, <a href="https://www.ctamericas.com/products-services/cloud-data-centers/idc-colocation/">https://www.ctamericas.com/products-services/cloud-data-centers/idc-colocation/</a> (accessed Mar. 1, 2019)	EB-561
29.		Cloud Infrastructure, China Telecom Americas, <a href="https://www.ctamericas.com/products-services/cloud-data-centers/enterprise-cloud-services/">https://www.ctamericas.com/products-services/cloud-data-centers/enterprise-cloud-services/</a> (accessed Mar. 1, 2019)	EB-565
30.		Managed CPE – China Telecom Americas, <a href="https://www.ctamericas.com/products-services/managed-services/managed-cpe/">https://www.ctamericas.com/products-services/managed-services/managed-cpe/</a> (accessed Mar. 1, 2019)	EB-569
31.		Managed Security, China Telecom Americas, <a href="https://www.ctamericas.com/products-services/managed-spervices/managed-security/">https://www.ctamericas.com/products-services/managed-spervices/managed-security/</a> (accessed Mar. 1, 2019)	EB-572
32.	X	June 13, 2018 Letter from DOJ National Security Division to China Telecom.	EB-576
33.	X	Aug. 30, 2018 E-mail from Morgan Lewis to DOJ National Security Division	EB-578

[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

34.	X	Sept. 18, 2018 E-mail from Morgan Lewis to DOJ National Security Division	EB-581
35.	X	Nov. 26, 2018 E-mail from Morgan Lewis to DOJ National Security Division	EB-585
36.	X	Dec. 6, 2018 Letter from Morgan Lewis to DOJ National Security Division with attachments	EB-589
37.	X	January 24, 2019 e-mail from Morgan Lewis to DOJ National Security Division	EB-655
38.		Developing a Trusted Security Strategy for China, China Telecom Americas, <a href="https://www.ctamericas.com/developing-security-strategy-for-china/">https://www.ctamericas.com/developing-security-strategy-for-china/</a> (accessed Mar. 23, 2019)	EB-658
39.		Privacy Policy, China Telecom Americas, <a href="https://www.ctamericas.com/privacy-policy/">https://www.ctamericas.com/privacy-policy/</a> (accessed Mar. 23, 2019)	EB-661
40.		<i>Fair Trade Comm'n v. Ruby Corp. et al.</i> , Case No. 16-cv-2438, Dkt. No. 1, Complaint at ¶ 31, 43-47 (D.D.C. filed Dec. 14, 2016)	EB-668
41.		<i>Fair Trade Comm'n v. Ruby Corp. et al.</i> , Case No. 16-cv-2438, Dkt. 9, Stipulated Order for Permanent Injunction and Other Equitable Relief (D.D.C. Dec. 19, 2016)	EB-684
42.		Screenshot, Financial, China Telecom Americas, <a href="https://www.ctamericas.com/industry-solutions/financial">https://www.ctamericas.com/industry-solutions/financial</a> (accessed Feb. 15, 2019)	EB-699
43.		Site Map, China Telecom Americas, cached July 2, 2017, <a href="https://web.archive.org/web/20170702035054/http://www.ctamericas.com/sitemap/">https://web.archive.org/web/20170702035054/http://www.ctamericas.com/sitemap/</a> (accessed Apr. 2, 2019)	EB-700
44.		<i>Intentionally blank</i>	EB-703
45.		<i>Intentionally blank</i>	EB-711
46.		<i>Intentionally blank</i>	EB-713
47.		<i>Intentionally blank</i>	EB-731
48.		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)	EB-732
49.		China Telecom Corp. Ltd., Annual Report (Form 20-F) (Apr. 28, 2016), Ex. 1.1 (Articles of Association of China Telecom Corp. Ltd. as of May 27, 2015)	EB-798
50.		The CEO of China Telecom is the latest Chinese executive to go 'missing,' Business Insider, <a href="https://www.businessinsider.com/china-telecom-ceo-chang-xiaobing-missing-in-corruption-crackdown-2015-12">https://www.businessinsider.com/china-telecom-ceo-chang-xiaobing-missing-in-corruption-crackdown-2015-12</a> (Feb. 28, 2015)	EB-864



**[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]**

51.		Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017), <a href="https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/">https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/</a>	EB-866
52.		<i>Intentionally blank</i>	EB-890
53.		China: New Regulation on Policy Cybersecurity Supervision and Inspection Powers issued, Library of Congress, <a href="http://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-inspection-powers-issued/">http://www.loc.gov/law/foreign-news/article/china-new-regulation-on-police-cybersecurity-supervision-and-inspection-powers-issued/</a> (Nov. 13, 2018)	EB-901
54.		China’s New Cybersecurity Measures Allow State Policy to Remotely Access Company Systems, Recorded Future Blog, <a href="https://www.recordedfuture.com/china-cybersecurity-measures/">https://www.recordedfuture.com/china-cybersecurity-measures/</a> (Feb. 8, 2019)	EB-903
55.		<i>Intentionally blank</i>	EB-913
56.		China Releases New Regulation on Cybersecurity Inspection, Inside Privacy, <a href="https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/">https://www.insideprivacy.com/data-privacy/china-releases-new-regulation-on-cybersecurity-inspection/</a> (Oct. 23, 2018)	EB-918
57.		National Cyber Strategy of the United States of America, White House at p.2, <a href="https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf">https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf</a> (September 2018)	EB-922
58.		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. (Dec. 12, 2018) (statement of John C. Demers, Assistant Attorney General, National Security Division, U.S. Department of Justice)	EB-962
59.		China’s Non-traditional Espionage Against the United States: The Threat and Potential Policy Responses at p. 1, Hearing Before the S. Comm. On the Judiciary, 115th Cong. (Dec. 12, 2018) (statement of Christopher Krebs, Director, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security)	EB-972
60.		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, <a href="https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF">https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF</a> (Mar. 22, 2018)	EB-978

**[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]**

61.		Update Concerning China's Acts, Policies and Practices Related to Technology Transfer, Intellectual Property, and Innovation at pp. 10-22, <a href="https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf">https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf</a> (Nov. 20, 2018)	EB-1193
62.		Significant Cyber Incidents, Center for Strategic and International Studies, <a href="https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity">https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity</a> (accessed Mar. 4, 2019)	EB-1246
63.		List of Significant Cyber Incidents Since 2006, Center for Strategic and International Studies, <a href="https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf">https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf</a> (accessed Mar. 4, 2019)	EB-1261
64.		Interactive Chart, Significant Cyber Incidents, CSIS Technology Policy Program, <a href="https://csis-ilab.github.io/js-viz/tech-policy/cyber-incidents-bar/index.html">https://csis-ilab.github.io/js-viz/tech-policy/cyber-incidents-bar/index.html</a> (accessed Mar. 4, 2019)	EB-1296
65.		Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2018, Office of the Secretary of Defense, <a href="https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF">https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF</a> (Aug. 16, 2018)	EB-1297
66.		Press Release, U.S. Department of Justice, Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies, <a href="https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading">https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading</a> (Oct. 10, 2018)	EB-1442
67.		Press Release, U.S. Department of Justice, Chinese Intelligence Officers and Their Recruited Hackers and Insiders Conspired to Steal Sensitive Commercial Aviation and Technological Data for Years, <a href="https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal">https://www.justice.gov/opa/pr/chinese-intelligence-officers-and-their-recruited-hackers-and-insiders-conspired-steal</a> (Oct. 30, 2018)	EB-1444
68.		Press Release, U.S. Department of Justice, PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage, <a href="https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage">https://www.justice.gov/opa/pr/prc-state-owned-company-taiwan-company-and-three-individuals-charged-economic-espionage</a> (Nov. 1, 2018)	EB-1446

[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

69.		Press Release, U.S. Department of Justice, Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information, <a href="https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion">https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion</a> (Dec. 20, 2018)	EB-1448
70.		Mandiant, APT1: Exposing One of China’s Cyber Espionage Units, <a href="https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf">https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf</a> (Feb. 19, 2013)	EB-1451
71.		Internet Vulnerability Takes Down Google, Thousand Eyes Blog, <a href="https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/">https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/</a> (Nov. 12, 2018)	EB-1527
72.		Press Release, China Telecom Corp. Ltd., Statement Regarding the Unfounded Report on China Telecom Being Alleged “Hijacking Internet Traffic,” <a href="http://www.irasia.com/listco/hk/chinatelecom/press/p181122.htm">http://www.irasia.com/listco/hk/chinatelecom/press/p181122.htm</a> (accessed Jan. 23, 2019)	EB-1535
73.		2010 Report to Congress, U.S.-China Economic and Security Review Commission at 243-44 (November 2010)	EB-1536
74.		Chinese ISP hijacks the Internet, BGPMon, <a href="https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/">https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/</a> (Apr. 8, 2010)	EB-1860
75.		Demchak, C. and Shavitt, Y, China’s Maxim – Leave No Access Point Unexploited: the Hidden Story of China Telecom’s BGP Hijacking, Military Cyber Affairs, Vol. 3: Iss. 1, Article 7 (2018)	EB-1866
76.		Facebook’s detour through China and Korea, BGPMon, <a href="https://bgpmon.net/facebooks-detour-through-china-and-korea/">https://bgpmon.net/facebooks-detour-through-china-and-korea/</a> (Mar. 26, 2011)	EB-1877
77.		D. Madory, China Telecom’s Internet Traffic Misdirection, VantagePoint Blog, <a href="https://dyn.com/blog/china-telecoms-internet-traffic-misdirection/">https://dyn.com/blog/china-telecoms-internet-traffic-misdirection/</a> (Nov. 5, 2018)	EB-1880
78.	X	Jan. 23, 2019 E-mail from Morgan Lewis to DOJ National Security Division	EB-1888
79.		China Telecom, PeeringDB, <a href="https://www.peeringdb.com/net/308">https://www.peeringdb.com/net/308</a> (accessed Feb. 8, 2019)	EB-1894

**[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]**

80.		FCC IBFS Search Results for "China Telecom," <a href="http://licensing.fcc.gov/myibfs/quickSearch.do?sortBy=callsign&amp;ssid=-97749747&amp;pgid=0">http://licensing.fcc.gov/myibfs/quickSearch.do?sortBy=callsign&amp;ssid=-97749747&amp;pgid=0</a> (accessed Mar. 7, 2019)	EB-1897
81.		Global Network, China Telecom Americas, <a href="https://www.ctamericas.com/company/global-network/">https://www.ctamericas.com/company/global-network/</a> (accessed Mar. 11, 2019)	EB-1899
82.		Foreign Economic Espionage in Cyberspace, National Counterintelligence and Security Center, <a href="https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace">https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace</a> (July 26, 2018).	EB-1903
83.		Company Overview, China Telecom Americas, <a href="https://www.ctamericas.com/company/company-overview/">https://www.ctamericas.com/company/company-overview/</a> (accessed Mar. 12, 2019)	EB-1923
84.		Xiruo Zhao, LinkedIn, <a href="https://www.linkedin.com/in/xiruo-zhao-361a9bb7/">https://www.linkedin.com/in/xiruo-zhao-361a9bb7/</a> (accessed Mar. 12, 2019)	EB-1927
85.		Office Locations, China Telecom Americas, <a href="https://www.ctamericas.com/office-locations/">https://www.ctamericas.com/office-locations/</a> (accessed Mar. 13, 2019)	EB-1936
86.		A. Robachevsky, 14,000 Incidents: a 2017 Routing Security Year in Review, <a href="https://www.manrs.org/2018/01/14000-incidents-a-2017-routing-security-year-in-review/">https://www.manrs.org/2018/01/14000-incidents-a-2017-routing-security-year-in-review/</a> (Jan. 9, 2018)	EB-1940
87.		China Telecom hijack of US Dept. of Energy route continuing into 6th day, <a href="https://twitter.com/internetintel/status/1080466509292621829">https://twitter.com/internetintel/status/1080466509292621829</a> (Jan. 2, 2019)	EB-1948
88.		Possible BGP hijack, <a href="https://bgpstream.com/event/171779">https://bgpstream.com/event/171779</a> (Dec. 28, 2018)	EB-1951
89.		K. Lougheed et al, A Border Gateway Protocol, RFC 1105 (Jun. 1989)	EB-1952
90.		Christopher Wray, Keeping our Financial Systems Secure: a Whole-of-Society Approach, Ninth Annual Financial Crimes and Cybersecurity Symposium, <a href="https://www.fbi.gov/news/speeches/keeping-our-financial-systems-secure-a-whole-of-society-response">https://www.fbi.gov/news/speeches/keeping-our-financial-systems-secure-a-whole-of-society-response</a> (Nov. 1, 2018)	EB-1970
91.	X	Sept. 17, 2018 E-mail from China Telecom to DOJ National Security Division	EB-1979
92.	X	Oct. 1, 2018 Letter from Morgan Lewis to DOJ National Security Division	EB-1983

[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

93.-		Press Release, Dept. of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage, First Time Criminal Charges are Filed Against Known State Actors for Hacking, <a href="https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor">https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor</a> (May 19, 2014)	EB-1986
94.		China Telecom Americas, CPNI Certification (Mar. 1, 2018), <a href="https://ecfsapi.fcc.gov/file/102283055404711/CHINA_T_ELECOM_AMERICAS_CPNI_CERTIFICATION_03_01_2018_SIGNED.PDF">https://ecfsapi.fcc.gov/file/102283055404711/CHINA_T_ELECOM_AMERICAS_CPNI_CERTIFICATION_03_01_2018_SIGNED.PDF</a>	EB-1990
95.		China Telecom Americas, CPNI Certification (Feb. 28, 2019), <a href="https://ecfsapi.fcc.gov/10228382226430/CHINA_TELECOM_AMERICAS_CPNI_CERTIFICATION_02_28_2019.pdf">https://ecfsapi.fcc.gov/10228382226430/CHINA_TELECOM_AMERICAS_CPNI_CERTIFICATION_02_28_2019.pdf</a>	EB-1995
96.	X	Mar. 21, 2019 Letter from DOJ National Security Division to Morgan Lewis	EB-2000
97.		<i>United States v. Xu</i> , No. 18-cr-43, Indictment (S.D. Ohio Apr. 4, 2018)	EB-2004
98.		<i>United States v. Zhang</i> , No. 13-cr-3132, Indictment (S.D. Cal. Oct. 25, 2018)	EB-2020
99.		<i>United States v. United Microelectronics Corp.</i> , No. 18-cr-465, Indictment (N.D. Cal. Sept. 27, 2018)	EB-2041
100.		<i>United States v. Zhu</i> , No. 18-cr-891, Indictment (S.D.N.Y. Dec. 17, 2018)	EB-2071
101.		Google goes down after major BGP mishap routes traffic through China, Ars Technica, <a href="https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/">https://arstechnica.com/information-technology/2018/11/major-bgp-mishap-takes-down-google-as-traffic-improperly-travels-to-china/</a> (Nov. 13, 2018)	EB-2094
102.	X	Mar. 21, 2019 Letter from DOJ National Security Division to Morgan Lewis	EB-2103
103.	X	Apr. 4, 2019 Letter from Morgan Lewis to DOJ National Security Division	EB-2107
104.		B. Marczak et al, Research Brief, China's Great Cannon, The Citizen Lab, <a href="https://citizenlab.ca/wp-content/uploads/2009/10/ChinasGreatCannon.pdf">https://citizenlab.ca/wp-content/uploads/2009/10/ChinasGreatCannon.pdf</a> (April 2015)	EB-2115

**[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]**

105.		J. Griffiths, When Chinese hackers declared war on the rest of us, MIT Technology Review, <a href="https://www.technologyreview.com/s/612638/when-chinese-hackers-declared-war-on-the-rest-of-us/">https://www.technologyreview.com/s/612638/when-chinese-hackers-declared-war-on-the-rest-of-us/</a> (Jan. 10, 2019)	EB-2134
106.		Screenshot of <a href="https://www.facebook.com/chinatelecomglobal/videos/st-even-tan-xu-president-of-china-telecom-america-corporation-shares-his-insight/940268502821658/">https://www.facebook.com/chinatelecomglobal/videos/st-even-tan-xu-president-of-china-telecom-america-corporation-shares-his-insight/940268502821658/</a> (June 1, 2018).	EB-2141
107.	X	April 18, 2019 Letter from Morgan Lewis to DOJ National Security Division	EB-2142
108.		Trans-Pacific Submarine Cable Systems, Submarine Networks, <a href="https://www.submarinenetworks.com/en/systems/trans-pacific/">https://www.submarinenetworks.com/en/systems/trans-pacific/</a> (April 19, 2019).	EB-2150
109.	X	March 27, 2019 Letter from Morgan Lewis to DOJ National Security Division	EB-2170
110.		<i>Federal Trade Comm'n v. Wyndham Worldwide Corp.</i> , CA No. 13-cv-1887, Dkt. No. 282-1 (Dec. 9, 2015)	EB-2171
111.		Network Operator Participants, Mutually Agreed Norms for Routing Security, <a href="https://www.manrs.org/isps/participants/">https://www.manrs.org/isps/participants/</a> (accessed May 1, 2019)	EB-2189
112.		China Telecom Corp. Ltd., Annual Report (Form 20-F), <a href="https://www.sec.gov/Archives/edgar/data/1191255/000119312519125555/d648641d20f.htm">https://www.sec.gov/Archives/edgar/data/1191255/000119312519125555/d648641d20f.htm</a> (filed on Apr. 29, 2019).	EB-2207
113.		Full text of resolution on amendment to CPC Constitution, State Council of the People's Republic of China, <a href="http://english.gov.cn/news/top_news/2017/10/24/content_281475919837140.htm">http://english.gov.cn/news/top_news/2017/10/24/content_281475919837140.htm</a> (Oct. 24, 2017)	EB-2379
114.		Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress, Article 33, <a href="http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf">http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf</a> (Oct. 24, 2017).	EB-2384
115.		Office of the Secretary of Defense, Annual Report to Congress: Military and Security Developments Involving the People's Republic of China (May 2, 2019)	EB-2412
116.		U.S. Trade Representative, 2018 Report to Congress on China's WTO Compliance (Feb. 2019).	EB-2548
117.		<i>Intentionally blank</i>	EB-2731

[[BUSINESS CONFIDENTIAL INFORMATION REDACTED]]

118.		China Law Translate, National Intelligence Law of the P.R.C. (2017), <a href="https://www.chinalawtranslate.com/en/tag/national-intelligence-law/">https://www.chinalawtranslate.com/en/tag/national-intelligence-law/</a> (accessed May 29, 2019).	EB-2735
119.	X	May 29, 2019 Letter from DOJ National Security Division to Morgan Lewis.	EB-2745
120.		Beijing's New National Intelligence Law, Lawfare Blog, <a href="https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense">https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense</a> (July 20, 2017).	EB-2747
121.		Doug Madory, <i>Large European Routing Leak Sends Traffic Through China Telecom</i> , Oracle Blog (June 6, 2019), <a href="https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom">https://blogs.oracle.com/internetintelligence/large-european-routing-leak-sends-traffic-through-china-telecom</a>	EB-2751
122.		Archana Kesavan, <i>WhatsApp Disruption: Just One Symptom of Broader Route Leak</i> , ThousandEyes Blog (June 7, 2019), <a href="https://blog.thousandeyes.com/whatsapp-disruption-just-one-symptom-of-broader-route-leak/">https://blog.thousandeyes.com/whatsapp-disruption-just-one-symptom-of-broader-route-leak/</a>	EB-2761
123.		Dan Goodin, <i>BGP event sends European mobile traffic through China Telecom for 2 hours</i> , Ars Technica (June 8, 2019), <a href="https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/">https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic-through-china-telecom-for-2-hours/</a>	EB-2768
124.	X	June 14, 2019 Letter from Morgan Lewis to DOJ National Security Division	EB-2774
125.	X	January 11, 2016 Letter from China Telecom to DOJ National Security Division, DHS and FBI	EB-2781