United States Senate
PERMANENT SUBCOMMITTEE ON INVESTIGATIONS
Committee on Homeland Security and Governmental Affairs

Rob Portman, Chairman
Tom Carper, Ranking Member

THREATS TO U.S. NETWORKS: OVERSIGHT OF CHINESE GOVERNMENT-OWNED CARRIERS

STAFF REPORT

PERMANENT SUBCOMMITTEE ON INVESTIGATIONS

UNITED STATES SENATE

THREATS TO U.S. NETWORKS: OVERSIGHT OF CHINESE GOVERNMENT-OWNED CARRIERS

TABLE OF CONTENTS

THREATS TO U.S. NETWORKS: OVERSIGHT OF CHINESE GOVERNMENT-OWNED CARRIERS

I. EXECUTIVE SUMMARY

Information and telecommunications technologies bring the world closer together, allowing individuals and businesses nearly everywhere in the world to communicate with each other. The expansion of global telecommunications networks, in particular, acts as a driving force of economic development by affording individuals unprecedented access to information and opportunities. Understanding the increasing interconnectedness of society, the Federal Communications Commission ("FCC")—the federal agency tasked with regulating the U.S. telecommunications industry—strives to open U.S. markets to foreign telecommunications carriers, where doing so is in the country's public interest. As a result, foreign-owned carriers have established operations within the United States.

Not all international expansion of telecommunications carriers, however, is in the United States' national security interests. Some foreign governments seek to exploit the openness of America's telecommunications market to advance their own national interests. One such country is China. The Chinese government views telecommunications as a "strategic" industry. It has expended significant resources to create and promote new business opportunities for its state-owned carriers and has established barriers to market entry for foreign carriers seeking to operate in China. Today, three state-owned carriers dominate the Chinese telecommunications market: China Mobile, China Telecom, and China Unicom, commonly referred to as the "Big Three." In addition to shoring up a stable domestic market for these carriers, the Chinese government has encouraged its carriers to expand into global markets, including the United States. This expansion, however, raises national security concerns. U.S. government officials have warned that Chinese state-owned carriers are "subject to exploitation, influence, and control by the Chinese government" and can be used in the Chinese government's cyber and economic espionage efforts targeted at the United States.

The operation of Chinese state-owned telecommunications carriers in the United States garnered public attention in May 2019 after the FCC denied China Mobile International (USA) Inc. ("China Mobile USA") the authority to provide international telecommunications services between the United States and foreign locations. The FCC premised its denial on national security concerns. This marked the first instance in which the FCC denied an application on national security grounds. Following that denial, the Subcommittee launched an investigation into how the U.S. federal government guards against risks posed by Chinese state-owned carriers already authorized to provide international telecommunications services between the United States and other points.

This report details how the U.S. federal government—particularly the FCC, Department of Justice ("DOJ"), and Department of Homeland Security ("DHS")—historically exercised minimal oversight to safeguard U.S. telecommunications networks against risks posed by Chinese state-owned carriers. Three Chinese state-owned carriers have been operating in the United States since the early 2000s, but only in recent years have the FCC, DOJ, and DHS focused on potential risks associated with these carriers. DOJ and DHS did enter into security agreements with two of the Chinese state-owned carriers prior to 2010, but they conducted only two site visits to each carrier since that time (or four total). Three of those visits occurred between 2017 and 2018. This lack of oversight undermined the safety of American communications and endangered our national security.

Since the Subcommittee launched its investigation, the agencies have increased their oversight of the Chinese state-owned carriers. The administration also recently issued an executive order establishing a formal committee to review the national security and law enforcement risks posed by foreign carriers operating in the United States. Still, the new committee's authorities remain limited, and as a result, our country, our privacy, and our information remain at risk.

* * * * *

The Chinese government exerts control over China's domestic telecommunications industry and state-owned carriers. China aims to be a world leader in technology by 2050, including in the telecommunications sector. To achieve this goal, China controls who can provide domestic services by maintaining one of the most restrictive foreign investment regimes in the world. Although the Chinese government may publicly state that it is opening the telecommunications market, foreign companies are subject to burdensome regulatory requirements; required to enter into joint ventures majority owned by Chinese parties; and often forced to transfer both technology and know-how to Chinese counterparts. State-owned carriers are equally controlled, as the Chinese government selects their management, sets target returns and growth rates, and compels companies to put state interests ahead of the carriers' market interests.

The Chinese government has encouraged state-owned telecommunications carriers to expand internationally. In 1999, the Chinese government issued a "Go Out" policy, through which it pledged financial support to entities to expand into global markets. Telecommunications carriers took advantage of this, with major state-owned carriers establishing operations across the world, including in the United States.

The Chinese government targets the United States through cyber and economic espionage activities and enlists state-owned entities in these efforts. Many U.S. government officials have highlighted the "persistent" threat posed by China.

As Assistant Attorney General of DOJ's National Security Division John Demers stated, China's "overall economic policy [is to] develop[ ] China at American expense." U.S. government officials have also warned that China will use its state-owned carriers to further its national interests. At least one Chinese carrier is publicly alleged to have hijacked and rerouted communications data through China. This allows Chinese actors to access sensitive communications, regardless of whether the data is encrypted.

* * * * *

The Subcommittee reviewed the federal agencies responsible for regulating and monitoring foreign telecommunications carriers operating in the United States. Although foreign carriers have operated in the United States for decades, the U.S. government had no statutory authorities to monitor the risks associated with these carriers. This is especially evident when reviewing the agencies' oversight of Chinese state-owned carriers.

The FCC regulates the U.S. telecommunications market. Carriers seeking to provide international telecommunications services between the United States and foreign points must apply for and obtain authorization from the FCC. The FCC's process is aimed at protecting the U.S. market from anti-competitive behavior in foreign markets. Thus, in evaluating applications, the FCC considers whether the foreign carrier's proposed services are in the public interest. Once authorization is granted, the Subcommittee found that it effectively exists in perpetuity; the FCC does not periodically review existing authorizations.

The FCC historically relied on "Team Telecom" to assess national security and law enforcement risks associated with a foreign carrier's provision of international telecommunications services. The FCC's public interest calculation involves weighing the national security, law enforcement, trade, and foreign policy implications associated with a foreign carrier's proposed services. The FCC has recognized, however, that it lacks the subject-matter expertise to evaluate these topics, and thus, it relies on certain Executive Branch agencies for guidance. For years, three agencies—DOJ, DHS, and the Department of Defense ("DOD"), which until recently were collectively referred to as "Team Telecom"—were tasked with evaluating national security and law enforcement concerns. Where Team Telecom believed that risks may exist, it attempted to mitigate those risks through a security agreement with the foreign carrier. These agreements provided Team Telecom with oversight capabilities, including the right to visit the carrier's U.S.-based facilities. If Team Telecom opted not to enter into a security agreement with a foreign carrier, it had no insight into the carrier's operations.

These measures were ineffective as Team Telecom lacked formal statutory authority, leaving its operations unstructured and *ad hoc*. Because of the lack of

statutory authority, Team Telecom had no formal, written processes for reviewing applications or monitoring compliance with security agreements. The informality also resulted in protracted review periods and a process FCC commissioners described as "broken" and an "inextricable black hole" that provided "no clarity for [the] future." For example, Team Telecom's review of China Mobile USA's application lasted seven years. Further, the agencies did not dedicate sufficient resources to ensure Team Telecom conducted oversight in an efficient and effective manner. The components of DHS and DOJ responsible for Team Telecom together historically tasked three employees with reviewing applications and monitoring compliance with security agreements.

In April 2020, as the Subcommittee was nearing the end of its investigation, the President issued Executive Order 13913, replacing the informal Team Telecom with the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services ("EO Telecom Committee"). The Executive Order seeks to address many of the shortcomings identified by the Subcommittee's investigation. The Executive Order requires members of the EO Telecom Committee to enter into a memorandum of understanding by July 3, 2020. Therefore, this report continues to refer to Team Telecom, even in relation to actions taken after April 4, 2020.

Beginning in 2018, Team Telecom and the FCC publicly highlighted the national security concerns associated with Chinese state-owned carriers operating in the United States. China Mobile USA's application marked the first instance in which Team Telecom recommended that the FCC deny a foreign carrier authorization to provide international telecommunications services on national security grounds. In its denial, the FCC relied on Team Telecom's conclusion that China Mobile USA is "subject to exploitation, influence, and control by the Chinese government." Such government control, Team Telecom warned, could advance the Chinese government's cyber and economic espionage activities targeted at the United States. Team Telecom specifically cautioned that China Mobile USA would build relationships with major U.S. carriers, through which it could gain access to U.S. networks and the sensitive public and private data transferred across those networks.

At least three other Chinese state-owned carriers have been operating in the United States for decades. The U.S. subsidiaries of the two other Big Three carriers—China Telecom and China Unicom—along with a smaller state-affiliated provider ComNet (USA) LLC ("ComNet") each received authorization to provide international telecommunications services in or prior to 2002 and have been operating ever since. During this time, these Chinese carriers have built relationships with major U.S. carriers and established points of presence across the United States. Further, China Telecom's U.S. subsidiary, China Telecom Americas, provides services to Chinese government facilities in the United States.

Until recently, Team Telecom conducted limited oversight of these Chinese state-owned carriers. Team Telecom entered into security agreements with China Telecom Americas (2007) and ComNet (2009), but it exercised minimal oversight over those entities until recently. During the more-than-ten year period in which these security agreements have been in effect, Team Telecom conducted just two site visits to each company—or four in total, three of which occurred within the past three years. At no point did Team Telecom enter into a security agreement with China Unicom Americas, meaning Team Telecom has no oversight authority to assess the company's operations in the United States.

The national security concerns Team Telecom and the FCC outlined in relation to China Mobile USA are applicable to the Chinese state-owned carriers currently operating in the United States. In advocating that the FCC deny China Mobile USA's application, Team Telecom raised a number of national security concerns related to China Mobile USA's Chinese government ownership. As Team Telecom officials acknowledged to the Subcommittee, those concerns also apply to China Telecom Americas, China Unicom Americas, and ComNet. The carriers are ultimately owned by the Chinese government; are required to comply with Chinese national security laws to support the Chinese government's intelligence work; and have established relationships with U.S. carriers, giving them access to critical infrastructure that the Chinese government could exploit in its economic and cyber espionage efforts. Team Telecom recognized these issues in its recent recommendation that the FCC to revoke China Telecom Americas' authorizations. The FCC also indicated its awareness of these concerns, when it recently called for all the carriers to demonstrate why their authorizations should not be revoked.

* * * * *

It must be noted that state-ownership does not presume a national security risk. Indeed, many foreign telecommunications companies around the world are state-owned. There are also compelling commercial interests dependent on facilitating the flow of data between the United States and China, which are among each other's top trading partners. The vast global telecommunications and technology infrastructure that facilitates commerce and economic development include undersea, terrestrial, wireless, and space-based networks jointly owned or operated by Chinese and Western companies.

Commercial interests, however, must be balanced against national security interests. Striking an appropriate balance between these interests requires the Executive Branch to exercise greater oversight and regularly evaluate the risks posed by foreign-owned companies, especially considering that national security concerns evolve over time. Currently, Chinese state-owned carriers are providing international telecommunications services based on FCC authorizations granted

more than a decade ago, in some cases nearly two decades. The carriers have provided services during this time, with minimal oversight from Team Telecom.

The Subcommittee's Investigations

This investigation continues the Subcommittee's examination of national security issues involving China. During the 115th Congress, the Subcommittee highlighted China's leading role in the opioid crisis by investigating how illicit opioids like fentanyl are shipped from China to the United States through international mail. The Subcommittee held an initial oversight hearing on May 25, 2017, titled "Stopping the Shipment of Synthetic Opioids: Oversight of U.S. Strategy to Combat Illicit Drugs." On January 25, 2018, the Subcommittee held a second hearing and issued a bipartisan report titled "Combatting the Opioid Crisis: Exploiting Vulnerabilities in International Mail." On October 24, 2018, the President signed into law the Synthetic Trafficking & Overdose Prevention Act ("STOP Act"), legislation designed to assist law enforcement in identifying and stopping fentanyl being shipped into the United States.

In the current 116th Congress, on February 28, 2019, the Subcommittee held a hearing and issued a bipartisan report titled "China's Impact on the U.S. Education System." The Subcommittee examined China's propaganda efforts at U.S. colleges and universities through Confucius Institutes. The Chinese government funds Confucius Institutes and hires Chinese teachers to teach language and culture classes to students and non-student community members. Confucius Institute funding comes with strings that can compromise academic freedom. The Chinese government approves all teachers, events, and speakers. Some U.S. schools contractually agree that both Chinese and U.S. laws will apply. The Chinese teachers sign contracts with the Chinese government pledging they will not damage Chinese national interests. The Subcommittee found that these limitations export China's censorship of political debate to the United States and prevent the academic community from discussing topics that the Chinese government believes are politically sensitive. In addition, a number of U.S. schools have been prevented from opening American cultural and educational centers in China. The Subcommittee recommended that, absent full transparency regarding how Confucius Institutes operate and full reciprocity for U.S. cultural outreach efforts on college campuses in China, Confucius Institutes should not continue in the United States. Twenty-one Confucius Institutes have closed since the Subcommittee published its report.

The Subcommittee continued its review of China's influence in the United States this congress by examining China's talent recruitment plans. On November 18, 2019, the Subcommittee released a bipartisan report titled "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans." The Subcommittee also held a hearing related to China's talent recruitment programs on November 19,

2019. The Subcommittee examined how American taxpayers have been unwittingly funding the rise of China's economy and military over the last two decades while federal agencies have done little to stop it. The Subcommittee found that China has been recruiting U.S.-based scientists and researchers and incentivizing them to transfer U.S. taxpayer-funded intellectual property to China for China's own military and economic gain. The Subcommittee focused specifically on China's most prominent talent recruitment program, the Thousand Talents Plan. The Subcommittee also surveyed seven federal agencies' efforts to combat the theft of American taxpayer-funded research and technology through Chinese talent recruitment programs, finding that the U.S. government does not have a comprehensive strategy to combat this threat.

At the November 19, 2019 hearing, the FBI's Assistant Director for Counterintelligence stated that "[w]ith our present-day knowledge of the threat from Chinese talent plans, we wish we had taken more rapid and comprehensive action in the past, and the time to make up for that is now." Following the Subcommittee's report and hearing, the Department of Justice has charged several individuals with crimes related to their participation in the Thousand Talents Plan, including the Chair of Harvard's Chemistry and Chemical Biology Department.

Finally, the Subcommittee has examined cyberattacks against U.S. companies that have been attributed to Chinese actors. On March 7, 2019, the Subcommittee released a bipartisan report titled "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach." The Subcommittee held a hearing on the report on March 7, 2019, which also examined the 2018 data breach suffered by Marriott. Chinese military personnel were indicted for their involvement in the Equifax breach on February 20, 2020, and Attorney General Barr indicated in announcing those indictments that Chinese government officials are also responsible for the attack against Marriott.

For this investigation, the Subcommittee reviewed more than 6,400 pages of documents and conducted more than 10 interviews, including interviews with individuals from the FCC, DOJ, DHS, China Telecom Americas, China Unicom Americas, ComNet, AT&T, Verizon, and CenturyLink. The Subcommittee also met with researchers who analyzed the Chinese government's use of telecommunications carriers to hijack communications. All entities and individuals complied with the Subcommittee's requests for information, documents, and interviews.

II. FINDINGS OF FACT AND RECOMMENDATIONS

Findings of Fact

(1) **The Chinese government exercises control over China's telecommunications industry and carriers.** The Chinese telecommunications market is the largest in the world, in terms of number of subscribers. The Chinese government views the telecommunications industry as critical and has set goals for the industry to "enter the ranks of powerful countries." To achieve this goal, the Chinese government exerts control over the domestic telecommunications market, including restraining foreign investment. Further, the largest domestic carriers are government owned; the Chinese government handpicks these firms' leaders, frequently shuffling the senior leadership between the companies. The carriers are also subject to "national service," requiring that they put State interests ahead of their commercial interests.

(2) **China does not provide U.S. telecommunications companies reciprocal access to the Chinese market and requires foreign carriers seeking to operate in China to enter into joint ventures with Chinese companies.** These joint ventures often require U.S. companies to give their technology, proprietary know-how, and intellectual property to their Chinese partners. In the two decades since China acceded to the World Trade Organization, "not a single foreign firm has succeeded in establishing a new joint venture" to access China's basic telecommunications services market and "only a few dozen foreign-invested suppliers have secured licenses to provide value-added telecommunications services, while there are thousands of licensed domestic suppliers."

(3) **The Chinese government encourages Chinese companies to take advantage of more open international markets.** Through its "Go Out" policy announced in 1999, the Chinese government provided financial support to state-owned companies to encourage expansion into global markets. Telecommunications carriers are among the companies that benefited, and they have since established operations across the world, including in the United States.

(4) **The Chinese government engages in cyber and economic espionage efforts against the United States and may use telecommunications carriers operating in the United States to further these efforts.** The U.S. government has highlighted the Chinese government's cyber and economic espionage efforts against the

United States. To carry out these efforts, the Chinese government frequently enlists the assistance of state-owned entities. Chinese state-owned companies are subject to an added layer of state influence in that they must comply with strict national security, intelligence, and cyber security laws regardless of where they operate. The U.S. National Counterintelligence and Security Center and the Director of National Intelligence have warned that the Chinese government is likely to use its state-owned carriers to assist in its espionage efforts because the carriers "provide valuable services that often require access to the physical and logical control points of the computers and networks they support." In fact, public reports allege that at least one Chinese carrier—China Telecom—and its affiliates have hijacked and rerouted data through China on a number of occasions since 2010. China Telecom and its affiliates, including its U.S. affiliate, China Telecom Americas, deny the public reports.

(5) The FCC regulates foreign carriers seeking to provide international telecommunications services between the United States and foreign points, but historically relied on Team Telecom to assess the national security and law enforcement risks associated with a foreign carrier's proposed services. The FCC also seeks input from other Executive Branch agencies concerning other risks, such as foreign policy and trade implications.

(6) The FCC is not required to review a foreign carrier's authorization after it has been granted. Authorizations effectively exist in perpetuity despite evolving national security implications. The FCC does not require a foreign carrier's authorization to be periodically reassessed to confirm the services continue to serve the public interest.

(7) Team Telecom was an informal group, with no statutory authority. As a result, its review of foreign carriers' applications was *ad hoc*, leading to delays and uncertainty. Throughout its existence, Team Telecom operated under no formal legislative or regulatory authority. Instead, it reviewed foreign carriers' applications at the request of and under the powers of the FCC. The lack of statutory authority resulted in a disorganized, haphazard, and lengthy review process that has been heavily criticized and referred to as an "inextricable black hole." Team Telecom had no deadlines by which it needed to make recommendations to the FCC, meaning the review of an application could—and often did—last years.

(8) The lack of statutory authority also prohibited Team Telecom from conducting meaningful oversight of foreign carriers authorized by the FCC. Team Telecom's monitoring and oversight capabilities existed only when it signed a security agreement with a foreign carrier. But, it was limited to monitoring compliance with the particular terms of the agreement. The stringency of these agreements increased over time, but historical agreements—particularly those entered before 2010—were written broadly, such that Team Telecom had little to verify. Further, Team Telecom did not start to develop an interagency process for monitoring compliance with security agreements until 2010 or 2011.

(9) Team Telecom had insufficient resources. DOJ and DHS historically dedicated fewer than five employees to reviewing applications and monitoring compliance with security agreements.

(10) Nearly a year after the Subcommittee began its investigation, the Administration issued an executive order that formalized Team Telecom. Executive Order 13913 established the EO Telecom Committee, set deadlines by which the EO Telecom Committee must complete reviews, and provided for input from other Executive Branch agencies, including the Intelligence Community. While the Order is a positive development, it does not address all of the concerns the Subcommittee identified relating to Team Telecom, including resource levels and formal review procedures.

(11) The FCC has authorized three Chinese state-owned carriers to provide international telecommunications services between the United States and foreign points. These three Chinese state-owned carriers have operated in the United States for decades: China Unicom Americas and China Telecom Americas obtained authorization in 2002; ComNet first obtained authorization in 1999.

(12) Team Telecom has had no interaction with China Unicom Americas since the FCC's authorization. Team Telecom has never sought a security agreement with China Unicom Americas, despite having opportunities to do so as recently as 2017. As a result, Team Telecom had no oversight of the company's operations in the United States.

(13) Team Telecom entered into security agreements with China Telecom Americas and ComNet, but conducted just two site visits in more than 10 years. Team Telecom entered into a security agreement with China Telecom Americas in 2007 and ComNet in 2009.

Since entering into the agreements more than ten years ago, Team Telecom conducted only two site visits to each company—or four in total. Only one of those visits occurred ***before*** 2017.

(14) The FCC and Team Telecom have recognized the national security risks posed by Chinese state-owned carriers operating in the United States. In particular, in connection with China Mobile USA's application, the FCC, Team Telecom, and other Executive Branch agencies cited three areas of concerns: (1) China Mobile USA could be exploited, influenced, and controlled by the Chinese government; (2) China Mobile USA could gain access to U.S. networks through interconnection arrangements with U.S. carriers; and (3) due to its Chinese government control and access to U.S. critical infrastructure, China Mobile USA could help the Chinese government in its cyber and economic espionage or other malicious activities. Team Telecom argued that, if authorized to provide international telecommunication services, China Mobile USA would have been able to monitor, degrade, and disrupt U.S. government communications. And, as a Chinese state-owned company, it must legally comply with requests made by the Chinese government and could not be expected to act against the interests of the Chinese government.

(15) The national security concerns outlined with respect to China Mobile USA apply to the other Chinese state-owned carriers operating within the United States. The carriers are ultimately owned by the Chinese government, and therefore subject to exploitation, influence, and control by the Chinese government. They may be forced to assist in cyber and economic espionage activities targeted at the United States, as they are similarly bound by Chinese national security laws. Further, the carriers have established relationships with major U.S. carriers, including AT&T, Verizon, and CenturyLink—all of which serve government entities, as well as private customers. China Telecom Americas also provides services to Chinese government facilities in the United States.

(16) Since the Subcommittee began its investigation, Team Telecom and the FCC took actions to address national security concerns posed by Chinese state-owned carriers. On April 9, 2020, Team Telecom recommended that the FCC revoke and terminate China Telecom Americas' authorizations. On April 24, 2020, the FCC issued a notice to each of the Chinese state-owned carriers requiring them to demonstrate why their authorizations should not be revoked.

Recommendations

(1) **The FCC should complete its review of China Telecom Americas, China Unicom Americas, and ComNet in a timely manner.** Team Telecom has recommended that China Telecom Americas' authorizations be revoked because of "substantial and unacceptable" national security concerns. The FCC should expeditiously review the authorizations of China Telecom Americas and the other Chinese state-owned carriers to ensure our national security and communications networks are not unnecessarily put at risk. As part of its review of China Unicom Americas' and ComNet's authorizations, the FCC should seek the recommendation of the newly established EO Telecom Committee as to national security and law enforcement concerns associated with the carriers' authorizations. The analysis should also include a decision as to whether risks can be mitigated—through the existing security agreements or new agreements.

(2) **The FCC should establish a clear standard and process for revoking a foreign carrier's existing authorizations.** Currently, there is no clear standard or process for revoking a foreign carrier's existing authorizations. Telecommunications companies must understand the circumstances under which authorizations could be revoked and be afforded due process to challenge potential revocation. Team Telecom officials indicated that they do not know what the FCC considers a "sufficient" basis for a revocation. Thus, while government officials may believe revocation is warranted, they may not recommend revocation without additional guidance. A formal standard and revocation process would provide clear guidance to both the government and industry as to when revocation of an existing authorization is warranted.

(3) **Congress should require the periodic review and renewal of foreign carriers' authorizations to provide international telecommunications services.** Currently, these authorizations can exist in perpetuity. Although the recent Executive Order allows the EO Telecom Committee to review existing authorizations, it does not *mandate* periodic review or renewal. Considering the limited resources DOJ and DHS dedicated to Team Telecom's review of foreign carriers' applications, it is unlikely that they will review many existing authorizations. National security and law enforcement concerns, as well as trade, and foreign policy concerns, however, are ever evolving, meaning that an authorization granted in one year may not continue to serve the public interest years later. Requiring a periodic review

and renewal of authorizations would ensure that the FCC and the Executive Branch continually account for evolving national security, law enforcement, policy, and trade risks.

(4) Congress should statutorily authorize the EO Telecom Committee. The Administration established the EO Telecom Committee, which formalizes Team Telecom, but the EO Telecom Committee still has no governing statutory authority. Team Telecom's historical lack of statutory authority led to a review process criticized by many as "opaque" and "broken." The recent Executive Order is a positive step, but formal legislative authority will provide for greater oversight over foreign carriers.

(5) Congress should preserve the role of other relevant Executive Branch agencies. Team Telecom was comprised of DOJ, DHS, and DOD officials. These agencies are also the primary components of the newly established EO Telecom Committee. Historically, the FCC has sought input on a foreign carrier's application from other Executive Branch agencies, including the Department of State, Department of Commerce, and the U.S. Trade Representative. The recent Executive Order makes these agencies, and others, advisors to the EO Telecom Committee. These agencies provide invaluable input and their role in the review process must be accounted for in any formal legislation.

(6) Congress should set deadlines by which decisions on FCC-related application reviews must be made. Team Telecom had no set deadlines by which it needed to complete its review of a foreign carrier's application pursuant to the FCC's request. Further, Team Telecom's already limited resources were often focused on actions related to the Committee on Foreign Investment in the United States ("CFIUS"). This resulted in protracted reviews and business uncertainty. Setting deadlines will imbue trust back into the review process. The recent Executive Order imposed certain timelines, but it allows for the EO Telecom Committee to seek extensions, which could draw out the review process, especially if resources remain limited.

(7) Congress should provide sustained resources necessary for the EO Telecom Committee to effectively assess foreign carriers' applications and to monitor foreign carriers operating in the United States. The Foreign Investment Risk Review Modernization Act of 2018 provided CFIUS agencies specialized authority to hire staff to ensure agencies can manage CFIUS filings. EO Telecom Committee agencies should be provided a similar authority to ensure it is able to

effectively and efficiently review foreign carriers' applications and monitor foreign carriers' operations.

(8) Congress should require the EO Telecom Committee to formally coordinate reviews of foreign carrier applications with CFIUS. The EO Telecom Committee's component agencies are members of CFIUS. CFIUS's and the EO Telecom Committee's processes overlap when a foreign investor seeks to acquire control of a U.S. telecommunications operator or infrastructure owner. These applications already undergo extensive review by CFIUS. Requiring formal coordination between CFIUS and the EO Telecom Committee will streamline the regulatory clearance process while meeting national security, law enforcement, trade policy, and foreign policy objectives.

(9) Congress should provide the EO Telecom Committee with authority to recommend revocation of a carrier's authorization, even where no security agreement exists between it and the carrier. Where no security agreement existed, Team Telecom did not interact with the foreign carrier. Although certain government officials believed that Team Telecom could review an existing authorization, even where no agreement existed, there is no formal, legal basis for such review. Combined with a requirement to periodically renew authorizations, affording the EO Telecom Committee the authority to review and recommend revocation of existing authorizations, even without a security agreement in place, allows the EO Telecom Committee to better respond to the evolving nature of national security risks.

(10) Congress should require the periodic review and renewal of security agreements between the EO Telecom Committee and foreign carriers. Team Telecom officials told the Subcommittee that, even if it believed that a security agreement was not comprehensive to address all risks associated with a foreign carrier's operations, it had little leverage to update the agreement. This means that certain risks, which could otherwise be mitigated, may go unaddressed. Requiring a periodic review and renewal of security agreements provides the EO Telecom Committee yet another tool to ensure that national security and other risks are regularly assessed and addressed.

(11) The EO Telecom Committee should establish formal, written policies and procedures governing its monitoring of compliance with security agreements. Team Telecom had no formal, written processes governing its monitoring of a foreign carrier's

compliance with a security agreement. It relied on written correspondence and site visits, but there was no clear method as to when these mechanisms were used or why. The EO Telecom Committee should document and formalize Team Telecom's processes, which will provide for more streamlined and consistent review of foreign carriers' operations in the United States.

(12) Congress and the Administration should take steps to ensure reciprocal access to the Chinese telecommunications market for U.S. companies. In those aspects of telecommunications in which China officially permits foreign participation, China requires forced technology transfers and imposes discriminatory regulatory processes and burdensome licensing and operating requirements. This results in a highly asymmetric playing field in which U.S. companies face immensely restrictive policies in China, while Chinese companies are not equally restricted in the United States.

III. BACKGROUND

This section discusses China's development of and control over its domestic telecommunications industry and carriers. In addition to exercising control over the domestic telecommunications industry, China has encouraged its carriers to expand internationally. During the past two decades, Chinese state-owned telecommunications carriers have established operations across the world, including in the United States. Finally, this section highlights the Chinese government's cyber and economic espionage efforts targeted at the United States and U.S. government officials' warnings about how the Chinese government may use its state-owned telecommunications carriers to further China's national interests.

A. China Views the Telecommunications Industry as Critical to National Priorities

The Chinese telecommunications market is the largest in the world, in terms of number of subscribers.[1] Telecommunications services in China are divided into two categories: basic telecommunications services ("BTS") and value-added telecommunications services ("VATS").[2] BTS provide "basic facilities of public networks, public data transmission as well as basic speech communication" and include services like fixed line and mobile calls, internet, international communication facilities, and satellite communications.[3] VATS include the "telecommunication and information services using the basic facilities of public networks" and includes e-mail and online data processing and database storage.[4]

In 2006, the Chinese government's State Council released the National Medium and Long-Term Program for Science and Technology Development, designating development of science and technology as a key Chinese strategic goal.[5] China aimed to become an "innovation-oriented country" by 2020 and a leader in science and technology by 2050.[6] To further this goal, China issued its Made in

---

[1] *China Telecommunications Market*, INT'L DATA CORP., https://www.idc.com/getdoc.jsp?containerId=IDC_P39849 ("In addition, in 2018, Chinese mobile subscribers reached 1.57 billion, which is the largest single mobile communication market in the world."); Dr. Daouda Cissé, *"Going Global" in Growth Markets—Chinese Investments in Telecommunications in Africa*, STELLENBOSCH UNIV. CENTRE FOR CHINESE STUDIES (2012).

[2] *See* Regulation Concerning Telecommunications of the People's Republic of China, Order of the State Council No. 291. Art. 8 (promulgated Sept. 25, 2000) (English translation), http://www.fdi.gov.cn/1800000121_39_2537_0_7.html.

[3] *Id.* at Art. 8, Appendix – Catalogue of Telecommunications Business.

[4] *Id.*

[5] Micah Springut, Stephen Schlaikjer & David Chen, *China's Program for Sci. & Tech. Modernization: Implications for American Competitiveness*, CENTRA TECH. INC. 6, 43 (Jan. 2011), https://www.uscc.gov/sites/default/files/Research/USCC_REPORT_China%27s_Program_forScience_and_Technology_Modernization.pdf (prepared for U.S.-CHINA ECON. & SEC. REVIEW COMM'N).

[6] JAMES MCGREGOR, U.S. CHAMBER OF COMMERCE, CHINA'S DRIVE FOR 'INDIGENOUS INNOVATION': A WEB OF INDUS. POLICIES 4, 17 (2010).

China 2025 ("MIC 2025") plan, which targets ten strategic industries deemed critical to China's economic competitiveness and high-tech growth.[7] According to the U.S. Chamber of Commerce, MIC 2025 "appears to provide preferential access to capital to domestic companies in order to promote their indigenous research and development capabilities, support their ability to acquire technology from abroad, and enhance their overall competitiveness."[8] The U.S. Chamber also found that, in concert with China's state-led development plans, MIC 2025 constitutes a "broader strategy to use state resources to alter and create comparative advantage[s] in these sectors on a global scale."[9]

The telecommunications industry is among those China deemed critical. In MIC 2025, the Chinese government outlines its goal for the information and telecommunications industry to "enter the ranks of powerful countries" by 2020.[10] China also seeks to be the leader in 5G international standards, technology, and industry and to reach 50 percent share of the international market for next generation internet.[11]

B. China Heavily Regulates its Telecommunications Industry and Carriers

To reach its goal to be a leader in the telecommunications industry, the Chinese government exerts control over foreign investment and domestic carriers. Further, it has incentivized state-owned carriers to expand operations internationally. This section analyzes each topic in turn.

1. China Heavily Restricts Foreign Telecommunications Investments

China maintains one of the most restrictive foreign investment regimes in the world.[12] The Chinese government first allowed foreign businesses in China during the 1970s.[13] Foreign investment accelerated in 2001, when—as a condition to join the World Trade Organization—China committed to allowing foreign carriers to form joint ventures with domestic carriers.[14] Despite the appearance of opening up, however, China has continued to restrict access to the telecommunications

---

[7] *See* U.S. CHAMBER OF COMMERCE, MADE IN CHINA 2025: GLOBAL AMBITIONS BUILT ON LOCAL PROTECTIONS 6 (2017).
[8] *Id.*
[9] *Id.*
[10] *Id.* at 65, 69.
[11] *Id.* at 66.
[12] *See id.* at 26 (citing OECD FDI Regulatory Index, http://www.oecd.org/investment/fdiindex.htm).
[13] Laney Zhang, *China: Foreign Investment Law Passed*, LIBRARY OF CONGRESS: GLOBAL LEGAL MONITOR (May 30, 2019), https://www.loc.gov/law/foreign-news/article/china-foreign-investment-law-passed/.
[14] WAYNE M. MORRISON, CONG. RESEARCH SERV., RL33536, CHINA-U.S. TRADE ISSUES 49–50 (2018).

sector.[15] Many telecommunications services remain "off-limits to foreign operators."[16] Instead, with limited exceptions,[17] foreign telecommunications companies must enter into joint ventures that are at least 50 percent owned by a Chinese party.[18]

The joint venture agreements often require U.S. companies to turn over their technology, proprietary know-how, and intellectual property to their Chinese partners, an exchange referred to as "forced technology transfer."[19] Former U.S. Treasury Secretary Timothy Geithner described the practice:

> We're seeing China continue to be very, very aggressive in a strategy they started several decades ago, which goes like this . . . you want to sell to our country, we want you to come produce here. If you want to come produce here, you need to transfer your technology to us.[20]

The European Union Chamber of Commerce in China reported in May 2019 that "results from its annual survey showed 20% of members reported being compelled to transfer technology for market access, up from 10% two years ago."[21] In addition, "nearly a quarter of those who reported such transfers said the practice was currently ongoing, while another 39% said the transfers had occurred less than

---

[15] OFFICE OF THE U.S. TRADE REPRESENTATIVE, EXEC. OFFICE OF THE PRESIDENT, FINDINGS OF THE INVESTIGATION INTO CHINA'S ACTS, POLICIES, AND PRACTICES RELATED TO TECH. TRANSFER, INTELLECTUAL PROP., & INNOVATION UNDER SECTION 301 OF THE TRADE ACT OF 1974 26, 28 (Mar. 22, 2018) [hereinafter 2018 U.S. TRADE REPRESENTATIVE REPORT].

[16] Yang Zhou, *Regulation of Telecommunications Sector in China: Overview*, ZHONG LUN (Aug. 16, 2017), http://www.zhonglun.com/Content/2017/08-16/1841302098.html#co_anchor_a836533_1.

[17] In 2019, the Chinese government removed restrictions on three categories of value-added telecommunications services: multi-party communication, store-and-forward, and call center businesses. Foreign ownership of businesses providing these services is now permitted. *See* Zoey Ye Zhang, *China's 2019 Negative Lists and Encouraged Catalogue for Foreign Investment*, CHINA BRIEFING (July 10, 2019), https://www.china-briefing.com/news/chinas-2019-negative-lists-encouraged-catalogue-foreign-investment/.

[18] *See* Regulations on the Administration of Foreign-Invested Telecommunications Enterprises, Art. 6 (promulgated Feb. 6, 2016), https://china.lexiscn.com/law/law-english-1-3161594-T.html?crid=1ffa565c-d660-b54d-6325-79b30208a4f5&prid= ("The proportion of capital contributed by the foreign investor(s) in foreign-funded telecommunications enterprise that is engaged in basic telecommunications services (other than radio paging services) shall not ultimately exceed 49%. The proportion of capital contributed by the foreign investor(s) in a foreign-invested telecommunications enterprise that is engaged in value-added telecommunications services (including radio paging business as part of its basic telecommunications services) shall not ultimately exceed 50%.").

[19] *See, e.g.*, KAREN SUTTER, CONG. RESEARCH SERV., IN11208, U.S. SIGNS PHASE ONE TRADE DEAL WITH CHINA 1 (2020); 2018 U.S. TRADE REPRESENTATIVE REPORT, *supra* note 15, at 19.

[20] WAYNE M. MORRISON, CONG. RESEARCH SERV., RL33536, CHINA-U.S. TRADE ISSUES 44 (2018). China publicly committed to rectifying this problem in 2016, but evidence indicates that the problem still exists. *Id*.

[21] Michael Martina, *China's Tech Transfer Problem is Growing, EU Business Group Says*, REUTERS (May 20, 2019).

two years ago."[22] Some researchers, however, suggest these percentages are under-inclusive given that Chinese officials often exert pressure to transfer technology orally to avoid creating a written record, and many companies avoid raising the issue to evade negative publicity or retaliation from the Chinese government.[23]

China's foreign investment approval process is also complex and variable. China imposes strict administrative licensing requirements for telecommunications carriers—they must secure approval from up to six government agencies before operating in the country.[24] This can include an anti-monopoly and national security review by the Ministry of Commerce; a review of the company's name by the State Administration of Industry and Commerce; and approval from the Ministry of Information Industry and Technology, China's telecommunications regulator.[25] Although the telecoms licensing approval timelines are officially either 60 or 180 days, depending on the type of license sought,[26] the overall approval process can last more than a year.[27] Complicating the bureaucratic licensing process is the discretion held by local officials, who may add unofficial requirements[28] and "impose deal-specific conditions in exchange for the licenses."[29]

These restrictions have blocked foreign carriers from accessing China's BTS market.[30] Since China's accession to the World Trade Organization almost two decades ago, "not a single foreign firm has succeeded in establishing a new joint venture to enter this sector."[31] China's VATS regulations have also "created serious barriers to market entry for foreign [carriers] seeking to enter this sector."[32] As a result, "only a few dozen foreign-invested [carriers] have secured licenses to value-added telecommunications services, while there are thousands of licensed domestic suppliers."[33] Although China has publicly agreed to lessen barriers for foreign

---

[22] *Id.*
[23] WAYNE M. MORRISON, CONG. RESEARCH SERV., RL33536, CHINA-U.S. TRADE ISSUES 44 (2018).
[24] *See* U.S. CHAMBER OF COMMERCE, CHINA'S APPROVAL PROCESS FOR INBOUND FOREIGN DIRECT INV. 10, chart 1 (2012).
[25] Specifics for the telecommunications industry are laid out in the Regulations on the Administration of Foreign-invested Telecommunications Enterprises (revised in 2016). *See also* U.S. CHAMBER OF COMMERCE, CHINA'S APPROVAL PROCESS FOR INBOUND FOREIGN DIRECT INV. 8–20 (2012) (listing other requirements).
[26] U.S. CHAMBER OF COMMERCE, CHINA'S APPROVAL PROCESS FOR INBOUND FOREIGN DIRECT INV. 8–20 (2012).
[27] 2018 U.S. TRADE REPRESENTATIVE REPORT, *supra* note 15, at 37.
[28] *See id.* at 20 (quoting an investigation submission that states, "Chinese officials are careful not to put such requirements in writing, often resorting to oral communications and informal 'administrative guidance' to pressure foreign firms to transfer technology").
[29] *Id.* at 39.
[30] OFFICE OF THE U.S. TRADE REPRESENTATIVE, EXEC. OFFICE OF THE PRESIDENT, NAT'L TRADE ESTIMATE REP. ON FOREIGN TRADE BARRIERS 119 (2020).
[31] *Id.*
[32] *Id.* (citing restrictions, including "opaque and arbitrary licensing procedures, foreign equity caps, and periodic, unjustified moratoria on the issuance of new licenses").
[33] *Id.*

investment in China,[34] numerous challenges remain.[35] China continues to "use discriminatory regulatory processes, informal bans on entry and expansion, case-by-case approvals, overly burdensome licensing and operating requirements, and other means to frustrate the efforts of U.S. suppliers of services to achieve their full market potential in China."[36]

2. China Exerts Control over Domestic Carriers

Not only does China limit foreign investment in the telecommunications industry, but it also controls its state-owned carriers. Prior to 1999, the Chinese government relied on a single carrier, which effectively had a monopoly on all telecom services in China.[37] However, the government chose to break up that monopoly and create a number of smaller, state-owned carriers to spur competition.[38] In 2008, the Chinese government reversed course and launched a series of reforms, which resulted in consolidating the number of carriers in China.[39]

Today, the Chinese telecommunications market is dominated by the "Big Three" carriers: China Mobile, China Telecom, and China Unicom.[40] The Chinese government controls the companies' management and operations.[41] "[M]ost senior executives of the Chinese telecom companies have links to the [Ministry of Information Industry and Technology], the Government, or the [Communist] Party."[42] The Chinese government handpicks the companies' leaders, frequently shuffling senior leadership between the companies, and implements policies discouraging intense competition between the Big Three.[43] In fact, in 2017, the

---

[34] *See* KAREN SUTTER, CONG. RESEARCH SERV., IN11208, U.S. SIGNS PHASE ONE TRADE DEAL WITH CHINA (2020).
[35] OFFICE OF THE U.S. TRADE REPRESENTATIVE, EXEC. OFFICE OF THE PRESIDENT, NAT'L TRADE ESTIMATE REP. ON FOREIGN TRADE BARRIERS 116 (2020).
[36] *Id.*
[37] James Huddleston, *The Battle between China's 3 Telecom Companies and Its Impact on Profits*, SEEKING ALPHA (July 23, 2013), https://seekingalpha.com/article/1565812-the-battle-between-chinas-3-telecom-companies-and-its-impact-on-profits.
[38] *Id.*
[39] Yukyung Yeo, *Between Owner and Regulator: Governing the Business of China's Telecommunications Service Industry*, 200 CHINA QUARTERLY 1013, 1023–24 (2009), https://www.jstor.org/stable/pdf/27756541.pdf.
[40] *See* Alan Weissberger, *China's Big 3 Mobile Operators Have 9 Million 5G Subscribers in Advance of the Service*; IEEE COMM. SOC. TECH. BLOG (Oct. 7, 2019), *https*://techblog.comsoc.org/2019/10/07/chinas-big-3-mobile-operators-have-9-million-5g-subscribers-in-advance-of-the-service-barrons-china-to-lead-in-5g-deployments/.
[41] *See, e.g.*, Bien Perez, *Bosses of China Mobile, Unicom and Telecom Reshuffled as Beijing Revamps State-Owned Telecommunications Firms*, SOUTH CHINA MORNING POST (Aug. 24, 2015).
[42] CHINA: TELECOM INDUSTRY BUSINESS OPPORTUNITIES HANDBOOK 1, 61 (2014).
[43] *China Telecom Chairman Moves to China Mobile*, THE ECONOMIST INTELLIGENCE UNIT (Mar. 6, 2019), http://www.eiu.com/industry/article/147729798/china-telecom-chairman-moves-to-china-mobile/2019-03-06; Huddleston, *supra* note 37.

government stated that it intended to factor in "social obligations" when selecting senior management for the Big Three carriers.[44]

The Chinese government also retains ultimate control over the carriers by setting target returns and growth rates.[45] State-owned carriers are subject to "national service," which compels them to put the government's development goals ahead of the companies' own market interests.[46] In 2017, for example, Li Keqiang, Premier of the Chinese Government, "directed China Mobile, China Unicom and China Telecom to remove all domestic long-distance and mobile roaming fees by the end of [the] year, significantly cut internet connection and leased line charges for small and medium-sized enterprises . . . and reduce international long-distance tariffs."[47] All three companies pledged to do so within 24 hours of the Premier's directive, despite noting that doing so would negatively impact their financial performance.[48]

3. China Encourages State-Owned Telecommunications Carriers to Expand Internationally

Although strictly regulating the domestic telecommunications industry, the Chinese government has also sought to take advantage of more open international markets. China formally announced a "Go Out" policy or "Going Global" strategy in 1999 to encourage state-owned enterprises to invest and expand overseas.[49] The Chinese government pledged financial support to companies in strategic industries to encourage expansion into global markets.[50] "The essence of the 'going global' strategy [was] to promote 'the international operations of capable Chinese firms with a view to improving resource allocation and enhancing their international competitiveness.'"[51] Other commentators noted that the underlying motive of the policy was to bolster "[Communist] Party claims to legitimacy by becoming an effective global actor."[52] Chinese telecom companies have benefited from this policy,

---

[44] Bien Perez, *Why Government Policy has a Bigger Impact on China's Telecoms Industry than Market Competition*, SOUTH CHINA MORNING POST (Mar. 11, 2017).
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] *See generally* NARGIZA SALIDJANOVA, U.S.-CHINA ECON. & SEC. REVIEW COMM'N, GOING OUT: AN OVERVIEW OF CHINA'S OUTWARD FOREIGN DIRECT INV. (Mar. 30, 2011).
[50] *See* Hongying Wang, *A Deeper Look at China's "Going Out" Policy*, CENTRE FOR INT'L GOVERNANCE INNOVATION (Mar. 8, 2016); NARGIZA SALIDJANOVA, U.S.-CHINA ECON. & SEC. REVIEW COMM'N, GOING OUT: AN OVERVIEW OF CHINA'S OUTWARD FOREIGN DIRECT INV. 5 (Mar. 30, 2011) (citing UNITED NATIONS CONFERENCE ON TRADE & DEV., WORLD INV. REPORT (2006)).
[51] NARGIZA SALIDJANOVA, U.S.-CHINA ECON. & SEC. REVIEW COMM'N, GOING OUT: AN OVERVIEW OF CHINA'S OUTWARD FOREIGN DIRECT INV. 5 (Mar. 30, 2011) (citing UNITED NATIONS CONFERENCE ON TRADE & DEV., WORLD INV. REPORT (2006)).
[52] CHINA POLICY, CHINA GOING GLOBAL: BETWEEN AMBITION AND CAPACITY 3 (Apr. 2017), https://policycn.com/wp-content/uploads/2017/05/2017-Chinas-going-global-strategy.pdf.

establishing operations abroad in an effort to acquire technology and new markets.[53]

C. The United States Government Has Highlighted National Security Concerns Associated with Chinese State-Owned Carriers Operating within the United States

In recent years, the U.S. government has highlighted national security concerns raised by China's state-owned telecom carriers operating in the United States. The U.S. National Counterintelligence and Security Center ("NCSC") notes that foreign telecom companies are often subject to foreign state influence because they "provide valuable services that often require access to the physical and logical control points of the computers and networks they support."[54] Chinese state-owned companies are subject to an added layer of state influence in that they must comply with strict laws regardless of where they operate.[55] These laws underscore the concern that the Chinese government may use state-owned carriers to assist in its cyber and economic espionage activities, particularly those targeted at the United States.[56]

This section discusses the Chinese government's history of cyber and economic espionage efforts against the United States. It then discusses some of the recent laws the Chinese government has enacted by which it could force companies to comply with Chinese government requests to assist in cyber and economic espionage efforts. Finally, this section discusses how a Chinese carrier might assist the Chinese government—through disrupting and rerouting internet and communications data. These "hijacking" efforts are possible because Chinese carriers have established operations in the United States and built interconnections with U.S. carriers.

---

[53] *Cf.* Dr. Daouda Cissé, *"Going Global" in Growth Markets—Chinese Investments in Telecommunications in Africa*, STELLENBOSCH UNIV. CENTRE FOR CHINESE STUDIES (2012).
[54] NAT'L COUNTERINTELLIGENCE & SEC. CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 14 (2018).
[55] *See, e.g.*, National Intelligence Law of the People's Republic, Art. 7 (adopted June 27, 2017), http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf (discussed *infra*).
[56] *See generally* 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 7 (filed July 2, 2018), https://licensing.fcc.gov/myibfs/download.do?attachment_key=1444739 [hereinafter *Executive Branch Recommendation re China Mobile USA*]; Redacted Executive Branch Recommendation to Revoke and Terminate China Telecom's International Section 214 Common Carrier Authorizations, FCC Nos. ITC-214-20010613-00346, ITC-214-20020716-00371, ITC-T/C-20070725-00285 (Apr. 9, 2020) [hereinafter *Executive Branch Recommendation re CTA*].

1. The Chinese Government Engages in Extensive Cyber and Economic Espionage Efforts against the United States

According to the NCSC, "foreign intelligence services—and threat actors working on their behalf—continue to" be the most persistent and pervasive cyber threat.[57] The NCSC concluded that China is among the most capable and active actors in this area, aggressively targeting and collecting sensitive economic and technological information to support its strategic development goals, including in the area of telecommunications.[58] Similarly, in the 2019 Worldwide Threat Assessment, the Director of National Intelligence warned that "China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems."[59] As Team Telecom recently highlighted, "China is the first country identified by name" in the 2019 Worldwide Threat Assessment given the threat it poses.[60]

The U.S. government is one of the leading targets of China's cyber espionage efforts.[61] A 2013 report by the Department of Defense concluded that China "is using its computer network exploitation . . . capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs."[62] Following the arrest of a Chinese officer on economic espionage charges, DOJ's National Security Division warned of China's "'overall economic policy of developing China at American expense,' often through illegal means."[63]

---

[57] NAT'L COUNTERINTELLIGENCE & SEC. CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 5 (2018).
[58] *Id.* ("China has expansive efforts in place to acquire U.S. technology to include sensitive trade secrets and proprietary information.").
[59] *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence*, 116th Cong. 5 (Jan. 29, 2019) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence).
[60] *Executive Branch Recommendation re CTA*, *supra* note 56, at 2 (citing *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence*, 116th Cong. 5 (Jan. 29, 2019) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence)).
[61] *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence* 6 (Feb. 13, 2018) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence) ("Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide.").
[62] U.S. DEP'T OF DEF., ANNUAL REPORT TO CONGRESS: MILITARY AND SECURITY DEVELOPMENTS INVOLVING THE PEOPLE'S REPUBLIC OF CHINA 36 (2013).
[63] Sam Karson, *Caught Between Superpowers: Alaska's Economic Relationship with China Amidst the New Cold War*, 36 ALASKA L. REV. 47, 56 (2019) (quoting John Demers, Assistant Attorney Gen., Nat'l Sec. Div., Dep't of Justice). *See also* Press Release, Dep't of Justice, Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies (Oct. 10, 2018), https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

Several instances demonstrate China's use of cyber espionage to attack U.S. government agencies and contractors to bolster its national security and economic priorities.[64] As part of China's "strategic plan" to increase its intelligence collection efforts, state-sponsored hackers have reportedly targeted U.S. networks containing large amounts of data on American intelligence personnel and government employees.[65] For example, in 2014, U.S. intelligence officials revealed that hackers associated with the Chinese government infiltrated Office of Personnel Management databases, which held personnel records and security-clearance files for former and current federal employees, their families, and friends; defense contractors' records were also obtained.[66] Over 22 million individuals were affected by the breach.[67] Former FBI Director Comey described the data as a "treasure trove of information about everybody who has worked for, tried to work for, or [currently] works for the United States government," making the breach a major national security concern.[68] Later that year, the Intelligence Community suspected that Chinese state-sponsored hackers were behind a breach of the U.S. Postal Service's computer networks—exposing data containing sensitive information on more than 800,000 employees.[69] Cyber policy experts concluded that the attack was part of the Chinese government's effort to build its inventory of information on U.S. persons for counter-intelligence and recruitment purposes.[70]

Chinese hackers have also targeted U.S. government contractors and the private sector. For example, in 2014, Chinese state-sponsored hackers allegedly breached the computer network of U.S. Investigation Services ("USIS"), which was then one of the government's largest contractors for providing federal background and security clearance investigations.[71] The breach resulted in the loss of more than 25,000 records belonging to DHS employees.[72] In 2018, Marriott's Starwood chain hotel reservation system was allegedly infiltrated by hackers working on

---

[64] *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence* 6 (Feb. 13, 2018) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence).
[65] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,* WASH. POST (July 9, 2015).
[66] *Id.*
[67] *The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation*, H.R. COMM. ON OVERSIGHT & GOV'T REFORM, MAJORITY STAFF REP., 114 Cong. 1, v n.1 (Sept. 7, 2016).
[68] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal Authorities Say,* WASH. POST (July 9, 2015).
[69] Ellen Nakashima, *China Suspected of Breaching U.S. Postal Service Computer Networks,* WASH. POST (Nov. 10, 2014).
[70] *Id.*
[71] Ellen Nakashima, *DHS Contractor Suffers Major Computer Breach, Officials Say,* WASH. POST (Aug. 6, 2014); Cory Bennett, *Report: China Hacked Security Contractor*, THE HILL (Nov. 3, 2014).
[72] Stephanie Stamm & Kaveh Waddell, *A Timeline of Government Data Breaches*, THE ATLANTIC (July 6, 2015).

behalf of China's Ministry of State Security.[73] The breach exposed personal information and travel details of up to 500 million people.[74] Earlier this year, DOJ charged four individuals associated with the Chinese People's Liberation Army for hacking Equifax in 2017.[75] As detailed in the Subcommittee's March 2019 report, the Equifax breach resulted in the release of personal identifying information of over 145 million Americans;[76] FBI Deputy Director Bowdich described it as "the largest theft of sensitive [personally identifying information] by state-sponsored hackers ever recorded."[77]

Pursuant to China's efforts to modernize its military and diminish the U.S. military's technological advantage, state-sponsored hackers have also engaged in a comprehensive campaign to steal information about U.S. advanced weapons technology.[78] For example, in 2012, a cyberattack on NASA's Jet Propulsion Laboratory was traced back to a Chinese IP address; during the incident the hackers "had full functional control over [the Laboratory's] networks."[79] Two years later, Chinese government-affiliated hackers stole military secrets, including the designs for Boeing's C-17 Globemaster and Lockheed Martin's F-35 and F22 stealth fighters.[80] More recently, Chinese state-sponsored hackers breached the computer network of a U.S. Navy defense contractor, stealing massive amounts of highly sensitive data, including secret plans for the development of a supersonic anti-ship submarine missile.[81]

---

[73] Ellen Nakashima, *U.S. Investigators Point to China in Marriot Hack Affecting 500 Million Guests,* WASH. POST (Dec. 11, 2018).
[74] *Id.*
[75] Criminal Indictment, United States v. Zhiyong et al., No. 2:20-CR046 (N.D. Ga. Jan. 28, 2020). *See also* Devlin Barrett & Matt Zapotosky, *U.S. Charges Four Chinese Military Members in Connection With 2017 Equifax Hack*, WASH. POST (Feb. 11, 2020).
[76] S. PERMANENT SUBCOMM. ON INVESTIGATIONS, HOW EQUIFAX NEGLECTED CYBERSECURITY AND SUFFERED A DEVASTATING DATA BREACH, 116 Cong. 1 (Mar. 6, 2019).
[77] Eric Geller, *U.S. Charges Chinese Military Hackers with Massive Equifax Breach*, POLITICO (Feb. 10, 2020).
[78] *See Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence* 6 (Feb. 13, 2018) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence). *See also China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses: Hearing Before the S. Comm. on the Judiciary*, 115 Cong. 3 (2018) (statement of Peter Harrell, Adjunct Senior Fellow, Center for a New Am. Sec.).
[79] *Investigating the Chinese Threat, Part I: Military and Econ. Aggression: Hearing before the H. Comm. on Foreign Affairs*, 112 Cong. 36 (2012) (statement of John J. Tkacik, Jr., Senior Fellow, Int'l Assessment & Strategy Center).
[80] Wendell Minnick, *Chinese Businessman Pleads Guilty of Spying on F-35 and F-22*, DEFENSE NEWS (Mar. 24, 2016), https://www.defensenews.com/breaking-news/2016/03/24/chinese-businessman-pleads-guilty-of-spying-on-f-35-and-f-22/.
[81] Ellen Nakashima & Paul Sonne, *China Hacks Navy Contractor and Secured a Trove of Highly Sensitive Data on Submarine Warfare*, WASH. POST (June 8, 2018).

China is also focused on commercial sectors critical to U.S. infrastructure, but vulnerable to cyberattack.[82] The U.S. Trade Representative recently warned that "cyber theft [was] one of China's preferred methods of collecting commercial information because of its . . . plausible deniability."[83] Many of the targeted companies operate in sectors that China believes are important for future innovation, such as information technology.[84] In 2014, then-Director of the National Security Agency, Admiral Michael Rogers, warned that China was capable of shutting down the U.S. electric grid and other critical infrastructure systems via cyberattack.[85] Just last year, cyber security experts attributed a cyberattack on the National Council of Examiners for Engineering and Surveying to Chinese state hacker-group APT10.[86] These experts warned that the attack was indicative of a specific threat to U.S. utility providers—the attacks were highly targeted and designed to steal intellectual property or to plant vulnerabilities in sectors essential to everyday national operations, such as energy, utilities, and telecommunications.[87]

China's cyber and economic espionage efforts are not expected to subside in the coming years. The Director of National Intelligence has advised that the Chinese government "will authorize cyber espionage against key U.S. technology sectors when doing so addresses a significant national security or economic goal not achievable through other means."[88] In a recent hearing before the Senate Committee on Homeland Security and Governmental Affairs, David J. Glawe, Undersecretary of the Office of Intelligence and Analysis at DHS, testified that China "will remain aggressive" in its cyber efforts against the United States and will continue to use its cyber capabilities to "undermine critical infrastructure, target our livelihoods and innovation, steal our national security secrets, and threaten our democratic institutions."[89]

---

[82] Zack Doffman, *Chinese State Hackers Suspected of Malicious Cyber Attack on U.S. Utilities*, FORBES (Aug. 3, 2019); U.S.-CHINA ECON. & SEC. REVIEW COMM'N, 2016 REPORT TO CONGRESS 1, 298–300 (Nov. 2016) (defining critical infrastructure to include the information technology sector).
[83] 2018 U.S. TRADE REPRESENTATIVE REPORT, *supra* note 15, at 153.
[84] COUNCIL ON FOREIGN RELATIONS, A NEW OLD THREAT: COUNTERING THE RETURN OF CHINESE INDUSTRIAL CYBER ESPIONAGE (Dec. 6, 2018).
[85] Ken Dilanian, *NSA Director: China Can Damage U.S. Power Grid*, ASSOCIATED PRESS (Nov. 20, 2014).
[86] Zack Doffman, *Chinese State Hackers Suspected of Malicious Cyber Attack on U.S. Utilities*, FORBES (Aug. 3, 2019).
[87] *Id.*
[88] *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence* 5 (Jan. 29, 2019) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence).
[89] *Threats to the Homeland: Hearing before the S. Comm. on Homeland Sec. & Governmental Affairs*, 116 Cong. (2019) (statement of David J. Glawe, Undersec'y, Office of Intelligence & Analysis, U.S. Dep't of Homeland Sec.).

2. Chinese State-Owned Companies are Subject to Control by the Chinese Government

China "enlist[s] the support of a broad range of actors spread throughout its government and industrial base" to carry out its strategic goals.[90] The Director of National Intelligence recently expressed concern about China's potential use of "Chinese information technology firms as routine and systemic espionage platforms . . . ."[91] In recent filings with the FCC, Team Telecom officials warned that Chinese telecommunications carriers, among other state-owned entities, are subject to control by the Chinese government because the entities must comply with strict national security laws.[92]

The Chinese government has enacted multiple laws obligating Chinese citizens and companies to support, assist, and cooperate in the government's intelligence and national security efforts.[93] The National Intelligence Law of 2017, for example, requires that all "organization[s] or citizen[s] shall support, assist and cooperate with the state intelligence work in accordance with the law, and keep the secrets of the national intelligence work known [*sic*] to the public."[94] The law also reserves the right for the state intelligence services to commandeer the communications equipment and other facilities of organizations and government organs.[95] The Chinese Cybersecurity Law of 2016, which became effective in June 2017, similarly provides that "network operators shall provide technical support and assistance to public security organs . . . ."[96] Under the 2015 National Security

---

[90] NAT'L COUNTERINTELLIGENCE & SEC. CTR., FOREIGN ECONOMIC ESPIONAGE IN CYBERSPACE 14 (2018).

[91] *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence* 4 (Jan. 29, 2019) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence).

[92] *See generally Executive Branch Recommendation re China Mobile USA*, *supra* note 56; *Executive Branch Recommendation re CTA*, *supra* note 56, at 38–40 (Apr. 9, 2020).

[93] *See* National Intelligence Law of the People's Republic, Art. 7 (adopted June 27, 2017), http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf. *See also* Murray Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE BLOG (July 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense. Other relevant Chinese laws obligating citizens and organizations to assist in "national security" efforts include the laws on Counterespionage (2014), National Security (2015), Counterterrorism (2015), and Cybersecurity (2016).

[94] National Intelligence Law of the People's Republic, Art. 7 (adopted June 27, 2017), http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

[95] *See id.* at Art. 17 ("According to the needs of the work, according to the relevant national regulations, the staff of the national intelligence work agency may preferentially use or legally requisition the means of transport, communication tools, sites and buildings of relevant organs, organizations and individuals . . . .").

[96] Cybersecurity Law of the People's Republic of China, Art. 28 (effective June 1, 2017), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. The law also requires "critical information infrastructure operators purchasing network products and services that might impact national security" to comply with a Government-led national security review. *See id.* at Arts. 35, 49. China Telecom Corporation

Law, all citizens and organizations are required to "obey[ ] . . . provisions of the Constitution, laws, and regulations regarding national security," "provid[e] conditions to facilitate national security efforts and other assistance," "provid[e] public security organs, state security organs or relevant military organs with necessary support and assistance," and "keep[ ] state secrets they learn of confidential."[97] The 2014 Counter-Espionage Law similarly provides that, during the course of a counter-espionage investigation, "relevant organizations and individuals shall truthfully provide information and must not refuse."[98]

Chinese companies operating in the United States have denied that they are bound by Chinese law.[99] Government officials and other commentators, however, point to the broad language of the laws to argue otherwise: the laws contain no geographic limitation and require that all organizations and citizens comply with requests from the Chinese government.[100] Further, while the laws are limited to "national security," "intelligence," and "counter-espionage" activities, these concepts are not defined.[101] Thus, commentators argue that the Chinese government could

---

Limited ("CTCL") has acknowledged that the 2017 Cybersecurity Law could require it to be subject to a "security review," which would be organized and conducted by China's Ministry of Industry and Information Technology and would "focus on the security and controllability of network products and services." CHINA TELECOM CORP. LTD. ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SEC. EXCH. ACT OF 1934 FOR THE FISCAL YEAR ENDED DECEMBER 31, 2019 (20-F), COMM. FILE NO. 1-31517, at 30 (filed Apr. 28, 2020), https://www.sec.gov/Archives/edgar/data/1191255/000119312520123302/d851335d20f.htm [hereinafter CHINA TELECOM FY2019 FORM 20-F].

[97] National Security Law of the People's Republic of China, Art. 77(1), (4)–(6) (adopted July 1, 2015), https://www.chinalawtranslate.com/2015nsl/?lang=en.

[98] *See* Counter-Espionage Law of the People's Republic of China, Art. 22 (adopted Nov. 1, 2014), https://www.chinalawtranslate.com/en/anti-espionage/.

[99] *See, e.g.*, Samantha Hoffman & Elsa Kania, *Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws*, AUSTRALIAN STRATEGIC POLICY INST. (Sept. 13, 2018), https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.

[100] *See* National Intelligence Law of the People's Republic, Art. 7 (adopted June 27, 2017), http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf; *5G: The Impact on National Security, Intellectual Property, and Competition: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. 2 (May 14, 2019) (testimony of Christopher Krebs, Dir., Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec.) ("Chinese laws on national security and cybersecurity provide the Chinese government with a legal basis to compel technology companies . . . to cooperate with Chinese security services."). *See also* Yuan Yang, *Is Huawei Compelled by Chinese Law to Help with Espionage*, FIN. TIMES (Mar. 4, 2019); AMNESTY INT'L, CHINA: SUBMISSION TO THE NPC STANDING COMM.'S LEGISLATIVE AFFAIRS COMM. ON THE DRAFT "NATIONAL INTELLIGENCE LAW" 4–5 (2017).

[101] *See* GOV'T OF CANADA, CHINA'S INTELLIGENCE LAW & THE COUNTRY'S FUTURE INTELLIGENCE COMPETITIONS, https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html; Yuan Yang, *Is Huawei Compelled by Chinese Law to Help with Espionage*, FIN. TIMES (Mar. 4, 2019); Samantha Hoffman & Elsa Kania, *Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws*, AUSTRALIAN STRATEGIC POLICY INST. (Sept. 13, 2018), https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-

use these provisions to justify instructions to state-owned carriers to engage in cyber and economic espionage on behalf of the Chinese government.[102] Further, given the state ownership, it is unlikely that the carriers would protest any such requests by the Chinese government.[103]

3. Chinese State-Owned Carriers Can Facilitate the Chinese Government's Espionage Efforts by Hijacking Data through Their Relationships with U.S. Carriers

Data transported across global networks are vulnerable to interception or interference by hostile actors.[104] The networks were created with minimal security, which allows malicious actors to "target, alter, block, and re-route" communications.[105] As the U.S. government has warned, "the deepening integration of the global telecommunications market has created risks and vulnerabilities in a sector replete with a broad range of malicious activities."[106] The telecommunications industry has been particularly susceptible to cyber espionage.[107] One report estimated that nearly half of telecommunications

---

espionage-laws/; AMNESTY INT'L, CHINA: SUBMISSION TO THE NPC STANDING COMM.'S LEGISLATIVE AFFAIRS COMM. ON THE DRAFT "NATIONAL INTELLIGENCE LAW" 4–5 (2017).

[102] *Cf. 5G: The Impact on National Security, Intellectual Property, and Competition: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. 2–3 (May 14, 2019) (testimony of Christopher Krebs, Dir., Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec.).

[103] *Cf.* Samantha Hoffman & Elsa Kania, *Huawei and the Ambiguity of China's Intelligence and Counter-Espionage Laws*, AUSTRALIAN STRATEGIC POLICY INST. (Sept. 13, 2018), https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/.

[104] *See, e.g.*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, U.S. DEP'T OF HOMELAND SEC., ALERT (TA16-250A): THE INCREASING THREAT TO NETWORK INFRASTRUCTURE DEVICES AND RECOMMENDED MITIGATIONS (last modified Sept. 28, 2016), https://www.us-cert.gov/ncas/alerts/TA16-250A ("The advancing capabilities of organized hacker groups and cyber adversaries create an increasing global threat to information systems. . . . For several years now, vulnerable network devices have been the attack-vector of choice and one of the most effective techniques for sophisticated hackers and advanced threat actors."). *Cf. 5G: The Impact on National Security, Intellectual Property, and Competition: Hearing Before the S. Comm. on the Judiciary*, 116th Cong. 1 (May 14, 2019) (testimony of Christopher Krebs, Dir., Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec.) ("Risks to mobile communications generally include such activities as call interception and monitoring, user location tracking, attackers seeking financial gain through banking fraud, social engineering, ransomware, identity theft, or theft of the device, services, or any sensitive data. . . . Risks to the mobile Data on 5G networks will flow through interconnected cellular towers, small cells, and mobile devices that may provide malicious actors additional vectors to intercept, manipulate, or destroy critical data. Malicious actors could also introduce device vulnerabilities into the 5G supply chain to compromise unsecured wireless systems and exfiltrate critical infrastructure data.").

[105] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 10.

[106] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 2–3.

[107] *See, e.g.*, *Critical Infrastructure and Communications Security*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/critical-infrastructure-and-communications-security ("The number of incidents of documented attacks on computer-based systems and communications systems increases on a daily basis. These range from unsophisticated access attempts by curious hackers to the

organizations were the target of malware attacks between 2017 and 2018,[108] and these organizations are increasingly subject to hijacking attacks, wherein third parties capture and reroute information.[109]

Hijacking attacks occur when information is routed from one point to another, usually when it is routed through different carriers' networks.[110] In routing, "information is sent across intervening [networks] as small data 'packets' with their destination IP addresses attached. Each router in the transited networks looks at the destination IP address in the packet and forwards it to the next and closest [network]," seeking the shortest and most efficient route from the start point to the end point.[111] The Border Gateway Protocol ("BGP") is the central routing protocol.[112] The BGP, however, is notoriously complex, and "errors can occur given the complexity."[113] It is these errors that open up opportunities for malicious actors to hijack traffic.[114]

---

malicious attempts to extract financial gain by criminal enterprises. The growth of malicious activities grew in the wake of the Telecommunications Act of 1996 as perpetrators capitalized on the 'openness' of networks, particularly the public Internet. The end result of these activities though can be catastrophic to the normal operations of communications and control systems and may threaten our national security."); *Worldwide Threat Assessment of the U.S. Intelligence Community Statement for the Record to the S. Select Comm. on Intelligence* 6 (Feb. 13, 2018) (statement of Daniel R. Coats, Dir. of Nat'l Intelligence) ("Most detected Chinese cyber operations against US private industry are focused on cleared defense contractors or IT and communications firms whose products and services support government and private sector networks worldwide."); *DNS Security—The Telecom Sector's Achilles' Heel*, EFFICIENTIP (Nov. 27, 2017), https://www.efficientip.com/dns-security-telecom-sector/ (finding that, per a 2017 survey, telecom organizations suffered more attacks than any other industry surveyed).

[108] Mike Robuck, *Report: Telecommunications Industry Woefully Unprepared for Cyberattacks*, FIERCETELECOM (Nov. 21, 2018).

[109] Jim Cowie, *The New Threat: Targeted Internet Traffic Misdirection*, DYN (Nov. 19, 2013), https://dyn.com/blog/mitm-internet-hijacking/; Juha Saarinen, *Internet Traffic Hijacking on the Rise*, ITNEWS (Nov. 21, 2013), https://www.itnews.com.au/news/internet-traffic-hijacking-on-the-rise-365006. "Hijack attacks expose a network to potentially critical damage because it is not a hack of the end-point but of the critical exchanges carrying information between end points." Yuval Shavitt & Chris C. Demchak, *China's Maxim—Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking*, 3 MILITARY CYBER AFFAIRS 1, 4 (2018).

[110] *See* U.S.-CHINA ECON. & SEC. REVIEW COMM'N, THE NAT'L SEC. IMPLICATIONS OF INVS. & PRODS. FROM THE PEOPLE'S REPUBLIC OF CHINA IN THE TELECOMM. SECTOR 42–43 (Jan. 2011); Shavitt & Demchak, *supra* note 109, at 4. Because different networks serve as the start and end points, a mechanism is needed to transport the traffic from one carrier to the other carrier for final delivery to the destination. Shavitt & Demchak, *supra* note 109, at 4.

[111] Shavitt & Demchak, *supra* note 109, at 2.

[112] *See, e.g.*, *What is BGP Hijacking*, CLOUDFLARE, https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/; Yashin Huang, *Internet Outrage Caused by Verizon Shows How Fragile the Internet Routing Is*, MEDIUM (July 2, 2019), https://medium.com/hackernoon/internet-outrage-caused-by-verizon-shows-how-fragile-the-internet-routing-is-a367241130e8. Administrators of each network are responsible for announcing the IP addresses associated with their networks on the BGP. *See, e.g.*, *What is BGP Hijacking*, CLOUDFLARE, https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/.

[113] Shavitt & Demchak, *supra* note 109, at 3.

[114] *See* Shavitt & Demchak, *supra* note 109, at 3.

In practice, if a malicious actor announces through the BGP that it owns an IP address block that actually is owned by Network 1, traffic destined for Network 1 will be routed to—or through—the malicious actor's network.[115] After receiving and inspecting the misdirected traffic, the malicious actor redirects it to the original destination point, and the traffic is delivered to its intended destination.[116] Because of the hijack, the malicious actor can access an organization's network, steal valuable data, add malicious implants to seemingly normal traffic, or simply modify or corrupt valuable data.[117] If diverted and copied even for a small amount of time, encryption can be broken.[118] Further, detecting the attack can be extremely difficult.[119] Given that traffic is continuously flowing, it is possible that the end-recipient might not notice any increase in "latency that results from the interception."[120]

Researchers allege that the Chinese government is increasingly using its state-owned telecommunications carriers to carry out hijacking attacks.[121] Chinese carriers have not established independent transmission facilities and networks outside of China.[122] Rather, as China Mobile stated in a recent SEC filing, the carriers are dependent on "interconnection arrangements and access to other networks."[123] Through these interconnection arrangements, the Chinese carriers can promote—and allegedly have promoted—false routes on the BGP.[124] Particular allegations of hijacking by Chinese state-owned carriers are discussed more below.

---

[115] *See What is BGP Hijacking*, CLOUDFLARE, https://www.cloudflare.com/learning/security/glossary/bgp-hijacking/.
[116] *See* Cowie, *supra* note 109.
[117] Shavitt & Demchak, *supra* note 109, at 4.
[118] Shavitt & Demchak, *supra* note 109, at 4.
[119] *See* Cowie, *supra* note 109; *BGP Hijacking Overview: Routing Incidents Prevention and Defense Mechanisms*, NOCTION (Apr. 24, 2018), https://www.noction.com/blog/bgp-hijacking.
[120] Cowie, *supra* note 109.
[121] *See, e.g.*, Doug Madory, *China Telecom's Internet Traffic Misdirection*, ORACLE: INTERNET INTELLIGENCE (Nov. 5, 2018), https://internetintel.oracle.com/blog-single.html?id=China+Telecom%27s+Internet+Traffic+Misdirection; Shavitt & Demchak, *supra* note 109, at 3; Jesus Diaz, *China's Internet Hijacking Uncovered*, GIZMODO (Nov. 17, 2010), https://gizmodo.com/chinas-internet-hijacking-uncovered-5692217; Andree Toonk, *Chinese ISP Hijacks the Internet*, BGPMON (Apr. 8, 2010), https://web.archive.org/web/20190415002259/https://bgpmon.net/chinese-isp-hijacked-10-of-the-internet/.
[122] *See, e.g.*, TT-DOJ-045–60; TT-DOJ-001–15.
[123] CHINA MOBILE LTD. ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SEC. EXCH. ACT OF 1934 FOR THE FISCAL YEAR ENDED DECEMBER 31, 2019 (FORM 20-F), COMM. FILE NO. 1-14696, at 16 (filed Apr. 28, 2020), https://www.sec.gov/Archives/edgar/data/1117795/000119312520122124/d825927d20f.htm#toc825927_5 [hereinafter CHINA MOBILE FY2019 FORM 20-F].
[124] *See, e.g.*, Shavitt & Demchak, *supra* note 109.

IV. EFFORTS TO MITIGATE NATIONAL SECURITY RISKS OF FOREIGN CARRIERS OPERATING IN THE UNITED STATES

This section analyzes the U.S. government's regulation of foreign carriers seeking or authorized to provide international telecommunications services between the United States and foreign destinations.[125] The FCC regulates the U.S. telecommunications market by authorizing foreign and domestic carriers to provide telecommunications services. As part of its analysis of whether to permit international telecommunications services, the FCC must determine that authorizing the carrier serves the public interest. This includes assessing a number of factors, including national security, law enforcement, foreign policy, and trade concerns raised by the proposed services. The FCC, however, does not analyze these factors itself. Instead, until recently, it relied on relevant Executive Branch agencies to provide subject-matter expertise on these topics. Team Telecom—an informal group comprised of DOJ, DHS, and DOD—was charged with assessing national security and law enforcement risks. But Team Telecom's review was historically described as "broken" and a "black hole," due in part to a lack of statutory authority and limited resources. Where Team Telecom did reserve for itself the right to monitor a foreign carrier's operations in the United States, it exercised that authority in an *ad hoc* manner.

A. The FCC Regulates the Operations of Foreign Telecommunications Carriers in the United States

The FCC is an independent[126] U.S. government agency responsible for regulating "interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories."[127] Congress created the FCC to evaluate and regulate competition within the communications industry and avoid economic waste, by assessing and preventing large monopolies and protecting existing carriers through regulation of market entry.[128] With a focus on ensuring economic opportunities, the FCC seeks to

---

[125] As described more below, this report focuses on carriers authorized to provide international telecommunications services under Section 214 of the Communications Act of 1934. International Section 214 authorization permits the authorization holder to provide international telecommunications services between the United States and foreign destinations. The FCC separately issues domestic Section 214 authorization for services within the United States. References to Section 214 authorization contained in this report are meant to refer to international Section 214 authorization, unless otherwise noted.

[126] The FCC is "an independent U.S. government agency overseen by Congress." It is "directed by five commissioners who are appointed by the President of the United States and confirmed by the U.S. Senate." *See What We Do*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/what-we-do.

[127] 47 U.S.C. § 151 et seq. (as amended) (2018); *Mission*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about/overview.

[128] *See generally* H. COMM. ON INTERSTATE & FOREIGN COMMERCE, COMMS. ACT OF 1934, SECTION 214 LEGISLATIVE BACKGROUND, H. DOC. NO. 44-667, 1–2 (1979) [hereinafter SECTION 214 LEGISLATIVE BACKGROUND].

promote "competition, innovation, and investment" in communications services and facilities.[129] The FCC's International Bureau administers "international telecommunications and satellite programs and policies, including licensing and regulatory functions,"[130] as well as monitors compliance "with the terms and conditions of authorizations and licenses granted by the Bureau . . .[,]" including authorizations to foreign carriers to operate telecommunications lines to, from, or within the United States.[131]

1. The FCC Authorizes Carriers to Provide Telecommunications Services in the United States Pursuant to Section 214 of the Communications Act of 1934

The FCC authorizes carriers to operate in the United States under Section 214 of the Communications Act of 1934.[132] Specifically, Section 214(a) provides that no telecommunications carrier may construct, extend, acquire, or operate a wire or cable line or engage in transmission over a line unless and until the FCC certifies that such action serves the public interest, convenience, and necessity.[133] Section 214 similarly regulates the transfer of control and assignment of telecommunication lines.[134]

The development of telecommunications technology in the early- and mid-1900s spurred the desire for greater government regulation of the industry.[135] Previously, oversight was effected through the Interstate Commerce Commission ("ICC"), although many viewed the ICC as only supervising routine matters and lacking an effective "legislative mandate to implement its mission."[136] A Department of Commerce interdepartmental committee ultimately recommended that the FCC be established to "centralize the jurisdiction of [the ICC] over wire and radio common carriers . . . and . . . over telegraph companies and telegraph lines."[137]

---

[129] *What We Do*, FED. COMMC'NS COMM'N, https://www.fcc.gov/about-fcc/what-we-do.
[130] *International*, FED. COMMC'NS COMM'N, https://www.fcc.gov/international. *See* 47 C.F.R. §§ 0.51, 0.261.
[131] *Functions of the International Bureau*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/international-bureau-functions. *See* 47 C.F.R. § 0.51.
[132] *See* 47 U.S.C. § 214(a).
[133] *See id.* FCC authorization is not required for "(1) a line within a single State unless such line constitutes part of an interstate line, (2) local, branch, or terminal lines not exceeding ten miles in length, or (3) any line acquired under section 221 [concerning consolidations and mergers of telephone companies]." *Id. See also* John Sallet, FCC General Counsel, *FCC Transaction Review: Competition and the Public Interest*, FCC BLOG (Aug. 12, 2014), https://www.fcc.gov/news-events/blog/2014/08/12/fcc-transaction-review-competition-and-public-interest.
[134] *See* 47 U.S.C. § 214(a).
[135] *See generally* SECTION 214 LEGISLATIVE BACKGROUND, *supra* note 128.
[136] SECTION 214 LEGISLATIVE BACKGROUND, *supra* note 128, at 25.
[137] SECTION 214 LEGISLATIVE BACKGROUND, *supra* note 128, at 25. Thus, the FCC regulates "common carriers," defined as "any person [partnership, association, joint-stock company, trust, or corporation] engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy . . . ." 47 U.S.C. § 153(11). Telecommunications

Section 214 served to codify this consolidation.[138] In presenting the proposed legislation, Representative Sam Rayburn, chairman of the sponsoring committee, summarized the purpose of Section 214 as follows:

> Section 214, relating to extensions of lines, is based upon section 1(18) – (22) of the Interstate Commerce Act, which relates only to transportation. It requires a certificate of public convenience and necessity from the Commission for the construction of a new interstate line . . . . The section is designed to prevent useless duplication of facilities, with consequent higher charges upon the users of the service.[139]

Today, Section 214 authorization covers a carrier's provision of "telecommunications services," defined as the "offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[140] The FCC's rules divide telecommunications services into (1) facilities-based services—where a carrier provides services across its own infrastructure and facilities,[141] and (2) resale services—where a carrier sells services provided through another carrier's network.[142]

2. The FCC Must Determine that International Section 214 Authorization Serves the Public Interest, but It Relies on the Executive Branch to Evaluate National Security, Law Enforcement, Foreign Policy, and Trade Concerns

The FCC's assessment of international Section 214 applications includes consideration of the applicant's foreign ownership, given that the FCC seeks to balance its desire for an open market against potential discrimination by foreign carriers against domestic carriers.[143] Prior to the mid-1990s, however, the FCC

---

carriers are separately defined as "any provider of telecommunications," with the exception of aggregators of telecommunications services, and are deemed to be common carriers to the extent that the carriers are providing telecommunications services. *See* 47 U.S.C. § 153(51).

[138] *See generally* SECTION 214 LEGISLATIVE BACKGROUND, *supra* note 128.

[139] SECTION 214 LEGISLATIVE BACKGROUND, *supra* note 128, at 26 (quoting 78 Cong. Rec. 10814 (1934)).

[140] *See* 47 U.S.C. § 153(53).

[141] *See* 47 C.F.R. § 63.22; Briefing with the Dep't of Justice (Apr. 3, 2020). Specifically, "facilities-based carrier" is defined as "a carrier that holds an ownership, indefeasible-right-of-user, or leasehold interest in bare capacity in the U.S. end of an international facility, regardless of whether the underlying facility is a common carrier or non-common carrier submarine cable or a satellite system." *See* 47 C.F.R. § 63.09(a).

[142] *See* 47 C.F.R. § 63.23; Briefing with the Dep't of Justice (Apr. 3, 2020).

[143] Paul W. Kenefick, *A Step in the Right Direction: The FCC Provides Regulatory Relief in International Settlements and International Services Licensing*, 8 COMM. LAW CONSPECTUS 45 (2000).

evaluated foreign ownership on an *ad hoc* basis.[144] Over time, the FCC formalized its international Section 214 application review process, including documenting the criteria it considers in evaluating applications.[145] The FCC has also taken a number of steps to streamline the process for reviewing and approving applications.[146]

When evaluating Section 214 applications, the FCC must determine that a carrier's proposed operations serve the public interest.[147] In 1995, the FCC explained that it considers a variety of factors when evaluating the public interest. Included among the factors are "national security, law enforcement issues, foreign policy, and trade concerns brought to [the FCC's] attention by the Executive Branch."[148] The FCC recognized that federal agencies have "specific expertise" in these matters, such that the FCC's analysis would benefit from those agencies' input.[149] It "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"[150] and "considers any such legitimate concerns as [it] undertake[s] [its] own independent analyses of whether grant of a particular authorization is in the public interest."[151] The carrier applicant has the burden to show that its proposed services would serve the public interest despite any national security, law enforcement, or other risks identified by the Executive Branch.[152]

Upon "accepting" an international Section 214 application, the FCC releases a public notice summarizing the applicant's proposed services.[153] Where a carrier

---

[144] *Id.*

[145] *See In the Matter of Mkt. Entry & Regulation of Foreign Affiliated Entities, Rep. & Order*, 11 FCC Rcd 3873 (1995) [hereinafter *1995 FCC Foreign Entry Order*]; *In the Matter of Streamlining the Int'l Section 214 Authorization Process & Tariff Requirements, Report & Order*, 11 FCC Rcd 12884 (1996) [hereinafter *1996 FCC Streamlining Order*]; 47 C.F.R. § 63.18. In 1999, the FCC granted all telecommunications carriers blanket authority under Section 214 to provide *domestic* interstate services and to construct or operate any *domestic* transmission lines. *Implementation of Section 402(b)(2)(A) of the Telecommunications Act of 1996 et al., Report and Order in CC Docket No. 97-11, Second Memorandum Opinion & Order in AAD File No. 98–43*, 14 FCC Rcd 11364, 11365–66, ¶ 2 (1999); 47 C.F.R. § 63.01.

[146] *See generally 1995 FCC Foreign Entry Order*, *supra* note 145; *1996 FCC Streamlining Order*, *supra* note 145.

[147] 47 C.F.R. § 63.18; 47 U.S.C. § 214; *1995 FCC Foreign Entry Order*, *supra* note 145, at ¶ 223; *In the Matter of Rules & Policies on Foreign Participation in the U.S. Telecomm. Mkt., Report & Order*, 12 FCC Rcd 23891, ¶¶ 65–66 (1997) [hereinafter *1997 FCC Foreign Participation Order*].

[148] *1995 FCC Foreign Entry Order*, *supra* note 145, at ¶ 3. *See also 1997 FCC Foreign Participation Order*, *supra* note 147, at ¶¶ 59–61.

[149] *1997 FCC Foreign Participation Order*, *supra* note 147, at ¶¶ 61–62. *See also 1995 FCC Foreign Entry Order*, *supra* note 145, at ¶¶ 38, 62, 216–19.

[150] *1997 FCC Foreign Participation Order*, *supra* note 147, at ¶ 63.

[151] *1997 FCC Foreign Participation Order*, *supra* note 147, at ¶ 62.

[152] *See In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3367, ¶ 11 (May 10, 2019).

[153] *See* 47 C.F.R. § 63.12(a). *See, e.g.*, Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-01338S (Jan. 16, 2009); Fed. Commc'ns Comm'n,

has a ten percent or greater foreign owner,[154] the FCC refers the application to the Executive Branch agencies via an "Executive Branch letter."[155] The letter explains that the FCC received an application from a carrier with foreign ownership interest and briefly describes the applicant and its proposed services.[156] The FCC requests that the agencies opine on whether the application raises national security, law enforcement, foreign policy, or trade policy concerns.[157] If the Executive Branch agencies do not raise national security, law enforcement, foreign policy, or trade policy concerns, the FCC conducts no further review of the issues.[158] In fact, in its Executive Branch letter, the FCC typically requests that agencies provide comments by a certain date, because the FCC is otherwise "prepared to take action on [the] application[ ]."[159] The FCC "streamlines" the application and deems it approved 14 days after the FCC issues a public notice of the application.[160] Thereafter, the carrier is allowed to begin providing the authorized services.

3. The FCC Does Not Periodically Review Section 214 Authorizations Once Granted

Once the FCC authorizes a carrier to provide services, nothing in the FCC's regulations require it to periodically renew that authorization or to reevaluate whether the carrier's services continue to serve the public interest.[161] As long as the authorized carrier pays annual regulatory fees, files regular reports, and otherwise complies with the FCC's rules, the authorization to operate and provide services

---

Public Notice – International Applications Accepted for Filing, Rep. No. TEL-00575S (Sept. 13, 2002); Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00417S (July 6, 2001); Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00144S (Oct. 13, 1999).

[154] NOTICE OF PROPOSED RULEMAKING: PROCESS REFORM FOR EXEC. BRANCH REVIEW OF CERTAIN FCC APPLICATIONS & PETITIONS INVOLVING FOREIGN OWNERSHIP, 31 FCC Rcd 7456, 7458 ¶ 6 (2016) [hereinafter FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM]. *See also Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 2; Kathleen Collins, Assistant Bureau Chief, International Bureau, Fed. Commc'ns Comm'n, Remarks for Panel Discussion at the 2d National Forum on CFIUS (July 21, 2015).

[155] *See* Briefing with the Dep't of Justice (Aug. 1, 2019). *See, e.g.*, FCC-PSI-000227–28; FCC-PSI-000478–79.

[156] *See* Briefing with the Dep't of Justice (Aug. 1, 2019). *See, e.g.*, FCC-PSI-000227–28; FCC-PSI-000478–79.

[157] *See, e.g.*, FCC-PSI-000227–28; FCC-PSI-000478–79.

[158] *See* Email from the Fed. Commc'ns Comm'n to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

[159] *See, e.g.*, FCC-PSI-000227–28; FCC-PSI-000478–79.

[160] *See* 47 C.F.R. § 63.12(a)–(b). In addition to requests by Team Telecom and other Executive Branch agencies, the FCC can remove an application from streamlining if certain specified regulatory requirements are met. *See id.*

[161] *See generally* 47 U.S.C. § 214(a). The FCC told the Subcommittee, however, that if at any time it finds an international Section 214 holder is not compliant with FCC rules, the FCC can and has referred the authorization holder to the FCC's Enforcement Bureau. Email from the Fed. Commc'ns Comm'n to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

effectively extends indefinitely.[162] A carrier can install, replace, or make other changes to its operations and equipment, so long as it does not impair the adequacy or quality of service provided.[163] A carrier can also use its international Section 214 authorization to demonstrate legitimacy of its operations in seeking interconnections with U.S. or other foreign carriers.[164] This means that a foreign carrier can operate for years, if not decades, at a time, without regard to the evolving global environment.

The FCC can revoke authorizations,[165] but the FCC has never done so under a national security standard.[166] The Subcommittee reviewed some FCC revocation decisions, which were based on the carrier discontinuing operations, ceasing to pay annual fees, or failing to file required reports, either with the FCC or Team Telecom.[167] One Team Telecom official suggested to the Subcommittee that, especially where a foreign carrier is servicing a large number of customers, the FCC may be hesitant to revoke an authorization because of the potential customer harm.[168]

---

[162] *See* 47 U.S.C. § 159(a); 47 C.F.R. § 63.20; *Fees*, FED. COMMC'NS COMM'N, https://www.fcc.gov/licensing-databases/fees.
[163] *See* 47 U.S.C. § 214(a).
[164] *See In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3377, ¶ 33 n.98 (May 10, 2019) (finding that Section 214 authorization would allow China Mobile USA to request interconnection with the networks of other Section 214-authorized U.S. common carriers).
[165] While there is no provision of the U.S. Code or the FCC's regulations that specifically provides for the revocation of international Section 214 authorizations, the FCC's prior revocation decisions generally cite to authority under 47 U.S.C. § 154(i) ("The Commission may perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this chapter, as may be necessary in the execution of its functions."). *See, e.g.*, *In the Matter of IP To Go, LLC*, 81 Fed. Reg. 91933 (Dec. 2016); *In the Matter of Redes Modernas de la Frontera SA de CV,* 81 Fed. Reg. 91932 (Dec. 2016); *In the Matter of JuBe Communications LLC,* 81 Fed. Reg. 55199 (Aug. 2016).
[166] *See* Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020). Although no decision has been reached, as described further below, the FCC recently ordered Chinese government-controlled carriers with international Section 214 authorizations to show cause why their authorizations should not be revoked. In the orders, the FCC highlighted national security concerns as a reason revocation may be warranted. *See* Press Release, Fed. Commc'ns Comm'n, FCC Scrutinizes Four Chinese Government-Controlled Entities Providing Telecommunications Services in the U.S. (Apr. 24, 2020), https://www.fcc.gov/document/fcc-scrutinizes-four-chinese-government-controlled-telecom-entities.
[167] Typically, Team Telecom alerts the FCC that the authorized carrier is failing to comply with the commitments outlined in the security agreement. Most instances reviewed by the Subcommittee involved a carrier that was no longer doing business in the United States and therefore was not filing the requisite information. Team Telecom recommended that the FCC terminate the authorization. The FCC first conducted its own lengthy review process, which included providing notice, allowing the applicant to respond to the allegations, and comply with the mitigation agreement. *See, e.g.*, *In the Matter of IP To Go, LLC*, 81 Fed. Reg. 91933 (Dec. 2016); *In the Matter of Redes Modernas de la Frontera SA de CV,* 81 Fed. Reg. 91932 (Dec. 2016); *In the Matter of JuBe Communications LLC,* 81 Fed. Reg. 55199 (Aug. 2016).
[168] Briefing with the Dep't of Justice (Aug. 1, 2019).

B. Team Telecom Assessed National Security and Law Enforcement Risks, but It Historically Operated in an *Ad Hoc* Manner

As described above, the FCC seeks input from a variety of Executive Branch agencies on the national security, law enforcement, foreign policy, and trade policy concerns implicated by a foreign carrier's Section 214 application.[169] DOJ, DHS, and DOD—until recently referred to as Team Telecom—focused on assessing national security and law enforcement risks.[170] DOJ's National Security Division's Foreign Investment Review Section served as the unofficial group lead for Team Telecom on Section 214 applications and coordinated among internal DOJ component parts and other Team Telecom members.[171]

Despite the long history of Team Telecom, it historically operated in an *ad hoc* manner. Team Telecom was not established in statute; it operated only at the request of the FCC.[172] Further, Team Telecom had no formal procedures, policies, or guidelines governing its review of Section 214 applications. This informality resulted in protracted review periods and a process FCC commissioners described as "broken,"[173] and an "inextricable black hole" that provided "no clarity for [the] future."[174] It also limited the actions Team Telecom could take to address identified national security or law enforcement risks. Team Telecom could recommend that the FCC approve or deny applications by foreign-owned entities.[175] Team Telecom

---

[169] *1997 FCC Foreign Participation Order*, *supra* note 147, at ¶ 63; FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 6. *See also Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 2.

[170] Briefing with the Dep't of Justice (Aug. 1, 2019); *Executive Branch Recommendation re CTA*, *supra* note 56, at 12. Other agencies, including the Department of State, the Department of Commerce, the United States Trade Representative, and the White House Office of Science and Technology Policy are responsible for assessing other concerns raised by the Section 214 application. *See* FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at n.16. Team Telecom works closely with the agencies to prepare a single recommendation on behalf of the Executive Branch, which is filed by the National Telecommunications and Information Administration, a part of the Department of Commerce. Briefing with the Dep't of Justice (Aug. 1, 2019). The Subcommittee's investigation focused on Team Telecom's processes. The Subcommittee, however, recognizes the important role played by the other agencies in evaluating risks associated with foreign carriers.

[171] Briefing with the Dep't of Justice (Aug. 1, 2019). Team Telecom also reviewed other applications at the request of the FCC, such as applications to operate submarine cable landing sites. For those applications, DHS's Office of Policy usually served as the lead coordinating agency. *See id;* Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

[172] Briefing with the Dep't of Justice (Aug. 1, 2019); Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

[173] *See* FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154 (statement, Ajit Pai, Commissioner, Fed. Commc'ns Comm'n).

[174] *See* Michael O'Reilly, *Team Telecom Reviews Need More Structure*, FED. COMMC'NS COMM'N (Sept. 18, 2015).

[175] Briefing with the Dep't of Justice (Aug. 1, 2019). *Cf.* FCC-PSI-003792–93 ("Executive Branch agencies have the opportunity to offer advice to the FCC regarding any foreign applicant seeking a

could also recommend a foreign-owned entity be approved for Section 214 authorization if it entered into a security agreement to mitigate national security or law enforcement concerns.[176] Even where a security agreement was entered, however, Team Telecom's process for monitoring compliance with that agreement was haphazard.

1. Team Telecom's Section 214 Review Process

Before the recent Executive Order, Team Telecom's process for reviewing foreign carriers' Section 214 applications was ambiguous, due in part to its lack of authority and established procedures. Team Telecom only publicly disclosed a list of factors it considered in evaluating national security and law enforcement concerns in 2018.[177] Upon receipt of the FCC's request to review a Section 214 application, Team Telecom conducted an initial review to determine whether the FCC's streamlining and granting of an application within two weeks was appropriate.[178] The factors weighed by Team Telecom included:

- The Applicant: Whether the applicant has a criminal history; has engaged in conduct that calls the applicant's trustworthiness into question; and is vulnerable to exploitation, influence, or control by other actors;

- State Control, Influence, and Ability to Compel Applicant to Provide Information: Whether an applicant's foreign ownership could result in the control of U.S. telecommunication infrastructure or persons operating such infrastructure by a foreign government; is from a country suspected of engaging in actions, or possessing the intention to take actions, that could impair U.S. national security; whether the applicant will be required, by virtue of its foreign ownership, to comply with foreign requests or is otherwise susceptible to such requests or demands made by a foreign nation or other actors; and whether such requests are governed by publicly available legal procedures subject to independent judicial oversight;

- Planned Operations: Whether the applicant's planned operations within the United States provide opportunities for an applicant or other actors to (1) undermine the reliability and stability of the domestic communications infrastructure, (2) identify and expose national security vulnerabilities, (3)

---

license to operate in the United States."); *1997 FCC Foreign Participation Order*, *supra* note 147, at ¶¶ 65–66.

[176] Briefing with the Dep't of Justice (Aug. 1, 2019).

[177] *Executive Branch Recommendation re CTA*, *supra* note 56, at 14–15; *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 6–7 (citing a May 2015 Letter from U.S. Dep't of Justice to China Mobile).

[178] Briefing with the Dep't of Justice (Aug. 1, 2019).

render the domestic communications infrastructure otherwise vulnerable to exploitation, manipulation, attack, sabotage, or covert monitoring, (4) 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 (5) otherwise engage in activities with potential national security implications; and

- U.S. Legal Process: 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.[179]

If no immediate concerns were identified, Team Telecom informed the FCC that it had no comment on or objections to the application.[180] As noted above, the FCC did not conduct further review of the issues—the foreign carrier's application was streamlined and deemed approved within 14 days.[181]

If Team Telecom determined that the applicant's foreign ownership or proposed services raised potential concerns, it recommended that the application be removed from the FCC's streamlining process.[182] Team Telecom also requested that the FCC defer any action on the application until Team Telecom's review was complete.[183] Team Telecom then engaged the foreign carrier applicant to learn more about its business and proposed services. Information solicited from the applicant typically included:

- Descriptions of the regulated and unregulated services provided by the applicant, including the technical specifications for providing such services;

---

[179] *Executive Branch Recommendation re CTA*, *supra* note 56, at 14–15; *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 6–7. According to Team Telecom, these factors were developed "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." *Executive Branch Recommendation re CTA*, *supra* note 56, at 15.

[180] Briefing with the Dep't of Justice (Aug. 1, 2019); FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 8; Kathleen Collins, Assistant Bureau Chief, International Bureau, Fed. Commc'ns Comm'n, Remarks for Panel Discussion at the 2d National Forum on CFIUS (July 21, 2015).

[181] *See* 47 C.F.R. § 63.12(a)–(b); FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 8; Kathleen Collins, Assistant Bureau Chief, International Bureau, Fed. Commc'ns Comm'n, Remarks for Panel Discussion at the 2d National Forum on CFIUS (July 21, 2015).

[182] Briefing with the Dep't of Justice (Aug. 1, 2019); Kathleen Collins, Assistant Bureau Chief, International Bureau, Fed. Commc'ns Comm'n, Remarks for Panel Discussion at the 2d National Forum on CFIUS (July 21, 2015).

[183] Briefing with the Dep't of Justice (Aug. 1, 2019); Kathleen Collins, Assistant Bureau Chief, International Bureau, Fed. Commc'ns Comm'n, Remarks for Panel Discussion at the 2d National Forum on CFIUS (July 21, 2015).

- Revenue information;

- Actual and expected categories of customers (e.g., enterprise, residential, carrier), including any federal, state, and local governmental customers;

- Individuals and entities with ownership interests and the level of each's involvement in the company;

- Members of management;

- Other foreign persons with access to infrastructure or customer records;

- Location of current and anticipated customer and business records; and

- Anticipated access to public switched telephone networks or the internet.[184]

Depending on the nature of the responses, Team Telecom occasionally required the applicant to clarify or expand on the information provided.[185] This engagement of the applicant was done solely by Team Telecom; no FCC personnel were involved.[186] Throughout this process, Team Telecom was constantly assessing whether its concerns could be mitigated through a written security agreement—commonly referred to as a network security agreement or a letter of assurance.[187] Team Telecom ultimately made one of three recommendations to the FCC:

1. It had no concerns and therefore no objection to the application;

2. Concerns existed but could be mitigated through a security agreement, so Team Telecom did not object to the FCC approving the application subject to the carrier agreeing to comply with the conditions and obligations contained in the security agreement; or

[184] *See, e.g.*, TT-DOJ-001–15; TT-DOJ-045–60; FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 7 (citing to a letter explaining that "the reviewing agencies' current practice is to send an applicant a set of initial questions").
[185] Briefing with the Dep't of Justice (Aug. 1, 2019); FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 7. *See also* TT-DOJ-106–08; TT-DOJ-061–63; TT-DOJ-067–101 (China Telecom Americas responding to Team Telecom's clarification questions about its Section 214 application).
[186] FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 7.
[187] FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 7; Briefing with the Dep't of Justice (Aug. 1, 2019). According to DOJ, there is no substantive difference between a network security agreement and a letter of assurance. *See* Briefing with the Dep't of Justice (Aug. 1, 2019). Thus, for ease of reference, the Subcommittee uses security agreement throughout.

3. The concerns were so great that they could not be mitigated by a security agreement and therefore, Team Telecom recommended that the application be denied outright.[188]

Where Team Telecom recommended the application be subject to the carrier complying with the conditions and obligations contained in a security agreement, the FCC's authorization provides that failure to comply with the conditions and obligations constitutes a failure to meet a condition of the Section 214 authorization and serves as grounds for terminating the authorization.[189]

2. Team Telecom's Lack of Statutory Authority, Established Procedures, and Limited Resources Hampered its Review Process

FCC Commissioners have long criticized Team Telecom's review process. Before becoming Chairman, Ajit Pai described the process as "broken," given that it "[took] too long and lack[ed] predictability."[190] Commissioner Michael O'Rielly similarly outlined a number of "high-level" complaints with Team Telecom's process, including:

- **Inextricable Black Hole** – Once applications are submitted, there is little to no information available to the [FCC], much less applicants, on status or potential areas of concern, no timeline for conclusion, and no way to discern which agency, if any, has concerns.

- **No Clarity for the Future** – The haphazard process does not provide any precedential value for future applicants to know what may be acceptable or unacceptable practices, structure or partnerships. This leaves applicants subject to the whim of the individual members of Team Telecom at that exact moment in time.[191]

One major criticism was the time Team Telecom took to review applications. Because its review process was not conducted pursuant to formal statutory

---

[188] *See* Briefing with the Dep't of Justice (Aug. 1, 2019). *See also* FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 8; Kathleen Collins, Assistant Bureau Chief, International Bureau, Fed. Commc'ns Comm'n, Remarks for Panel Discussion at the 2d National Forum on CFIUS (July 21, 2015).

[189] *See, e.g., IB Public Notice*, 30 FCC Rcd at 11018; *Wypoint Telecom, Inc., Termination of International Section 214 Authorization, Order*, 30 FCC Rcd 13431, 13431–32, ¶ 2 (2015). In addition to termination, the FCC can impose monetary sanctions or other enforcement actions for failing to meet a condition of the authorization. 47 U.S.C. §§ 312, 503.

[190] *See* FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154 (statement, Ajit Pai, Commissioner, Fed. Commc'ns Comm'n).

[191] *See* Michael O'Reilly, *Team Telecom Reviews Need More Structure*, FED. COMMC'NS COMM'N (Sept. 18, 2015), https://www.fcc.gov/news-events/blog/2015/09/18/team-telecom-reviews-need-more-structure.

authority, once an application was removed from streamlining, Team Telecom had no deadline by which it had to make a final recommendation to the FCC.[192] Therefore, the process could—and did—last years. In response to an FCC notice of proposed rulemaking, telecommunications companies claimed that applications referred to Team Telecom took up to four times longer to process than other applications.[193] As discussed more below, China Mobile USA applied for Section 214 authorization in September 2011, but Team Telecom did not recommend that the FCC deny that application until July 2018.[194]

Current officials recognize that Team Telecom has suffered from a lack of statutory authority.[195] Although the Department of Justice served as the unofficial lead, Team Telecom had no formal chair or spokesperson.[196] Further, both internally and externally, Team Telecom had to work with agencies that had conflicting responsibilities and mission areas.[197] This often led to interagency delay in decision making.[198] As one Team Telecom component agency characterized, "responsibility without authority is problematic."[199]

Team Telecom's review process also suffered from a lack of staff dedicated to reviewing applications. DHS officials estimated that the Office of Policy, which represents DHS on Team Telecom, has had, at most, only two employees designated to Team Telecom; these employees are responsible for all aspects of the Team Telecom portfolio, including reviewing applications and monitoring compliance with security agreements.[200] DOJ historically dedicated only one attorney to Team

---

[192] *See* Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).
[193] Comments of Telecommunications Companies, IB Docket No. 16-155, at 4 (May 23, 2016) ("FCC applications requiring referral to Team Telecom . . . take three to four times longer to receive approval than applications not subject to this review.").
[194] *See Int'l Bureau Selected Applications Listing, File No. ITC-214-20110901-00289*, FED. COMMC'NS COMM'N, http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITC2142011090100289&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number.
[195] Briefing with the Dep't of Justice (Aug. 1, 2019); Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Apr. 3, 2020); Email from the Dep't of Justice to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[196] Briefing with the Dep't of Justice (Aug. 1, 2019); Briefing with the Dep't of Justice (Apr. 3, 2020); Email from the Dep't of Justice to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[197] Briefing with the Dep't of Justice (Aug. 1, 2019); Briefing with the Dep't of Justice (Apr. 3, 2020); Email from the Dep't of Justice to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[198] *Cf.* Briefing with the Dep't of Justice (Aug. 1, 2019); Briefing with the Dep't of Justice (Apr. 3, 2020).
[199] Email from the Dep't of Justice to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[200] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020). This does not account for employees from other DHS offices, such as the Office of General Counsel, who assist on Team Telecom matters. *See* Email from Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).

Telecom matters.[201] Like DHS, DOJ's employee was responsible for both the initial review of applications and post-authorization compliance monitoring.[202] With limited exception, these individuals were responsible not only for Team Telecom's portfolio but also that of the Committee on Foreign Investment in the United States ("CFIUS").[203] Because the CFIUS process is governed by statutory requirements, including deadlines by which applications must be reviewed, DOJ and DHS resources typically focused on those projects, at the expense of Team Telecom projects.[204] DOJ claims to have vastly increased its Team Telecom resources in recent years. Today, it has five attorneys dedicated to reviewing FCC applications.[205] According to the team's managing attorney, however, the longest tenured individual has been with the agency for little more than a year.[206]

3. Team Telecom's Post-Authorization Monitoring and Oversight Was Also Limited and Sporadic

Not only was Team Telecom's review of Section 214 applications limited, but so too was its oversight and monitoring of the carriers with which it entered into a security agreement.[207] Without a security agreement, Team Telecom had no insight into the activities of a foreign-owned carrier after Section 214 authorization was granted.[208] Team Telecom officials informed the Subcommittee that they believed they had the authority to review any Section 214 authorized carrier at any time, even where no security agreement existed.[209] The officials further noted their belief that Team Telecom could recommend that the FCC revoke an existing authorization at any time.[210] However, the officials acknowledged there was no formal legal basis for these reviews and recommendations, and Team Telecom never conducted a *sua sponte* review or recommended revoking the authorization of a carrier with which Team Telecom did not have a security agreement.[211]

Where Team Telecom did enter into a security agreement with a Section 214 authorized carrier, Team Telecom had a slightly larger degree of oversight power.[212] Team Telecom's authority, however, was limited to ensuring the carrier complied

---

[201] Briefing with the Dep't of Justice (Apr. 3, 2020).
[202] *Id.*
[203] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).
[204] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).
[205] Briefing with the Dep't of Justice (Apr. 3, 2020).
[206] *Id.*
[207] Briefing with the Dep't of Justice (Aug. 1, 2019).
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*
[212] *Id.*

with the specific terms of the security agreement.[213] Team Telecom officials, however, recognized the limited enforcement mechanism this provides.[214] Although security agreements have become more robust over time, older agreements contained few provisions, were broad in scope, and provided little for Team Telecom to verify.[215] Another reason that monitoring agreements proved difficult is that Team Telecom had to rely heavily on the carrier's forthrightness:

> Although [Team Telecom] . . . monitors [a company's] compliance with [its security] agreements on an ongoing basis, [Team Telecom] can never have full visibility into all of a company's activities. Therefore, [Team Telecom] necessarily relies on the other party to adhere rigorously and scrupulously to [security] agreement provisions and to self-report any problems or issues of non-compliance.[216]

Team Telecom retained oversight authority through the security agreements; however, its exercise of that authority was sporadic.[217] Team Telecom did not establish a process by which to ensure compliance with security agreements until 2010 or 2011, even though it entered into agreements years prior.[218] Team Telecom developed no formal protocol, policy, or guidance document detailing how it monitored compliance with security agreements.[219] Team Telecom officials stated it relied heavily on written correspondence and requests for information from the foreign carriers.[220] Team Telecom provided no evidence or explanation demonstrating how it evaluated written representations for accuracy.

Team Telecom also conducted site visits to the carriers' U.S.-based facilities. It used these visits to physically visit domestic sites, look for violations of a security agreement, and speak to employees.[221] As with written correspondence, the frequency of site visits varied.[222] Further, even if Team Telecom identified violations of the security agreement or issues to suggest the security agreement was inadequate, Team Telecom did not have strong enforcement mechanisms.[223] It

---

[213] *Id.*
[214] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).
[215] *Id.*
[216] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 16.
[217] Although never formally documenting its compliance monitoring procedures, the Department of Justice noted that it has always dedicated personnel to compliance monitoring. Historical knowledge about these compliance efforts, however, has been "weakened" due to employee attrition. *See* Email from the Dep't of Justice to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[218] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020). Around 2010, the Department of Homeland Security created an internal interagency system of record to track Team Telecom compliance deliverables, which is still used today. *Id.*
[219] Briefing with the Dep't of Justice (Aug. 1, 2019).
[220] *Id.*
[221] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).
[222] Briefing with the Dep't of Justice (Aug. 1, 2019).
[223] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

could attempt to induce companies to come back into compliance with agreement terms or recommend that the FCC revoke a carrier's authorization.[224] Team Telecom officials, however, claimed they do not know what the FCC would deem a sufficient reason for revocation, and none were familiar with the FCC ever revoking an authorization on the basis of national security concerns.[225] Team Telecom officials, however, stressed that site visits were still a helpful tool in that they, at a minimum, signaled to the foreign carriers that Team Telecom was watching from an oversight perspective.[226]

As with the review process, in addition to limited statutory authority,[227] resources have been a major contributing factor to Team Telecom's haphazard oversight.[228] As described above, DHS has only two employees dedicated to Team Telecom—both reviewing applications and monitoring security agreement compliance.[229] DOJ historically had one attorney doing the same.[230] Although it has attempted to increase resources, DOJ currently employs only two attorneys dedicated to compliance monitoring efforts.[231] Those attorneys, along with their supervisor, are responsible for monitoring compliance with more than 100 security agreements.[232]

C. Nearly a Year after the Subcommittee's Investigation Began, the Administration Took Steps to Formalize Team Telecom

Nearly a year after the Subcommittee launched its investigation and extensively engaged with members of Team Telecom, the administration took steps to address systemic issues regarding Team Telecom. On April 4, 2020, the President issued Executive Order 13913, formalizing Team Telecom as the Committee for the Assessment of Foreign Participation in the United States

---

[224] *Id.*; Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[225] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).
[226] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).
[227] Team Telecom officials noted that the lack of statutory authority left it with limited enforcement mechanisms. For example, unlike CFIUS, Team Telecom had no subpoena authority or means to protect classified information. *See* Email from the Dep't of Justice to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[228] *See id.*
[229] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020). Again, this represents only employees in DHS's Office of Policy, which is the DHS representative to Team Telecom. It does not include employees from other DHS offices, such as the Office of General Counsel, who assist on Team Telecom matters. *See* Email from Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[230] Briefing with the Dep't of Justice (Apr. 3, 2020).
[231] *Id.*
[232] *Id.*

Telecommunications Services Sector ("EO Telecom Committee").[233] DOJ officially leads the EO Telecom Committee, which also includes DHS and DOD; other Executive Branch agencies, including the Intelligence Community, serve as advisors.[234] The EO Telecom Committee is tasked with "assist[ing] the FCC in its public interest review of national security and law enforcement concerns that may be raised by foreign participation in the United States telecommunications services sector."[235] To that end, the EO Telecom Committee is authorized to review Section 214 and other applications, respond to any risks presented by the applications, and recommend dismissal, denial, modification, or revocation of an authorization.[236] It is also permitted—but not required—to review existing authorization.[237]

Unlike Team Telecom's historical operations discussed above, where the timeline for application review was not standardized, the Executive Order provides that any initial application review must be completed "before the end of the 120-day period beginning on the date the [Attorney General] determines that the applicant's responses to any questions and information requests from the Committee are complete."[238] Thus, before the clock begins to run, DOJ must determine that all of its questions have been satisfactorily answered.[239] This can take—and in some instances, such as those described below, has taken—months. Where the EO Telecom Committee determines that a "secondary assessment" is warranted, the Executive Order requires such an assessment be completed in 90 days.[240]

The Executive Order establishes timelines and assigns roles. It does not, however, address the entirety of past concerns regarding Team Telecom. Notably, the Executive Order does not afford the EO Telecom Committee any additional resources; it provides only that DOJ shall "provide such funding and administrative support for the Committee" as may be required.[241] As described above, DOJ's current staffing ignores the realities necessary to effectively and efficiently assess Section 214 applications and to monitor compliance with security agreements. Further, the Executive Order permits, but does not require, the review of Section 214 authorizations where no security agreement exists. Finally, the Executive Order provides no clarity regarding what may trigger a security agreement or a recommendation to deny an application.

---

[233] Exec. Order No. 13913, 85 C.F.R. § 19643 (Apr. 4, 2020).
[234] *Id.* at §§ 3(b)–(d).
[235] *Id.* at § 3(a).
[236] *Id.*
[237] *Id.* at § 6.
[238] *Id.* at § 5(b)(iii).
[239] *Id.*
[240] *Id.* at § 5(c).
[241] *Id.* at § 11(b).

V. CHINESE STATE-OWNED TELECOM COMPANIES OPERATED IN THE UNITED STATES WITH MINIMAL OVERSIGHT FROM THE FCC AND TEAM TELECOM

The FCC's and Team Telecom's limitations described above resulted in a lack of oversight of Chinese state-owned carriers operating in or seeking to operate in the United States. In 2018, Team Telecom acknowledged that Chinese state-owned telecommunications carriers providing international telecom services between the United States and foreign points raise national security concerns.[242] This occurred in connection with Team Telecom's first ever recommendation to deny Section 214 authorization because of national security concerns: the application of Chinese state-owned carrier China Mobile USA.[243] The recommendation, however, came *seven* years after the application was submitted.[244] The FCC waited another year before denying the application in 2019.[245]

Three Chinese state-owned carriers currently possess international Section 214 authorizations: (1) China Telecom (Americas) Corporation ("CTA"); (2) China Unicom (Americas) Operations Limited ("CUA"); and (3) ComNet (USA) LLC ("ComNet") (and its immediate parent company Pacific Networks Corp.). All three companies received Section 214 authorizations nearly two decades ago and have operated in the United States since.[246] Team Telecom officials acknowledged to the

---

[242] *See Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3; *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361 (May 10, 2019).

[243] *See Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3; *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3365 (May 10, 2019); Press Release, Fed. Commc'ns Comm'n, FCC Denies China Mobile USA Application to Provide Telecommunications Services (May 9, 2019), https://docs.fcc.gov/public/attachments/DOC-357372A1.pdf ("This is the first instance in which Executive Branch agencies have recommended that the FCC deny a section 214 application due to national security and law enforcement concerns.").

[244] *See Int'l Bureau Selected Applications Listing, File No. ITC-214-20110901-00289*, FED. COMMC'NS COMM'N, http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITC2142011090100289&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number.

[245] *See id.* During the year period, China Mobile USA and Executive Branch agencies were provided opportunities to file arguments in favor of and against denial. The FCC told the Subcommittee that staff "actively worked on the recommendation to deny from July 2018, when it was received" until the May 2019 order. It also suggested that it took longer to reach a decision because the "denial of an international Section 214 application on national security grounds was a case of first impression." *See* Email from the Fed. Commc'ns Comm'n to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

[246] *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00581, DA No. 02-2500, 17 FCC Rcd 19181, 19182 (Oct. 3, 2002) (CUA authorization); Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00567, DA 02-2060, 17 FCC Rcd 16199, 16201 (Aug. 22, 2002) (CTA authorization); *Fed. Commc'ns Comm'n, Public Notice – International Authorizations Granted*, Rep. No. TEL-00423, DA No. 01-1794, 16 FCC Rcd 14695, 14696 (July 26, 2001) (China Telecom authorization); *Fed. Commc'ns Comm'n, Public*

Subcommittee that there is no meaningful difference between the services for which China Mobile USA sought authorization to provide and the services currently being provided by the three other Chinese state-owned carriers.[247] Further, the officials stated that CTA, CUA, and ComNet were also susceptible to the same national security and law enforcements concerns Team Telecom raised when recommending the FCC deny China Mobile USA's application.[248] Nevertheless, until recently, Team Telecom conducted minimal oversight of these entities, despite having entered into security agreements with CTA and ComNet more than a decade ago.[249] During that time, Team Telecom conducted only two site visits to each company.[250] Team Telecom, by contrast, never entered into a security agreement with CUA, meaning it has had no interaction with the company.[251] Only since April 2020, when the Subcommittee was nearing the end of its investigation, did Team Telecom and the FCC take steps to fully assess whether the companies' existing authorizations continue to serve the public interest.[252]

A. China Mobile Limited and China Mobile USA

China Mobile Limited ("China Mobile") is "the leading provider of telecommunications and related services in Mainland China."[253] The company provides a full suite of communications services, including "mobile voice and data business [and] wireline broadband."[254] Together with its subsidiaries, it is also the

---

Notice – International Authorizations Granted, Rep. No. TEL-00151, DA No. 99-2328, 14 FCC Rcd 17862, 17864 (Oct. 28, 1999) (ComNet authorization).

[247] Briefing with the Dep't of Justice (Apr. 3, 2020); Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

[248] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).

[249] *See* Letter from Yi-jun Tan, President, China Telecom (USA) Corp., to Sigal Mandelker, Deputy Assistant Att'y Gen., Dep't of Justice, Elaine Lammert, Deputy Gen. Counsel, Fed. Bureau of Investigation, & Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec. (July 17, 2007); Letter from Norman Yuen, Chairman, Pacific Networks Corp., & Fan Wei, Dir., CM Tel (USA) LLC to Stephen Heifetz, Deputy Assistant Sec'y for Policy Dev., Dep't of Homeland Sec. & Matthew Olsen, Acting Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Justice (Mar. 3, 2009).

[250] *See* DHS00472PSI–76; DHS00477PSI–89; DHS00460PSI–65; DHS00466PSI–71; TT-DOJ-521–73; TT-DOJ-495–99; TT-DOJ-500–06; TT-DOJ-507–20.

[251] Briefing with China Unicom Americas (Apr. 16, 2020); Briefing with the Dep't of Justice (Apr. 3, 2020); Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).

[252] *See Executive Branch Recommendation re CTA*, *supra* note 56; Press Release, Fed. Commc'ns Comm'n, FCC Scrutinizes Four Chinese Government-Controlled Entities Providing Telecommunications Services in the U.S. (Apr. 24, 2020), https://www.fcc.gov/document/fcc-scrutinizes-four-chinese-government-controlled-telecom-entities. Team Telecom officials stressed to the Subcommittee that, although it did not file its recommendation to revoke CTA's authorizations until April 2020, it was reviewing CTA's authorizations long before that. Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).

[253] CHINA MOBILE FY2019 FORM 20-F, *supra* note 123, at 21.

[254] *About China Mobile – Overview*, CHINA MOBILE LIMITED, https://www.chinamobileltd.com/en/about/overview.php.

largest provider of telecommunications services in the world, as measured by the total number of subscribers,[255] with approximately 946 million mobile customers worldwide as of March 2020.[256] China Mobile reported a 2019 operating revenue of $107 billion, of which approximately 90 percent came from telecommunications services.[257]

Outside of China, China Mobile operates through its subsidiary, China Mobile International.[258] China Mobile USA, a subsidiary of China Mobile International, was registered in Delaware in May 2011; it maintains offices in New York and California.[259]

On September 1, 2011, China Mobile USA applied for Section 214 authorization to provide international facilities-based and resale services between the United States and all international points, including China.[260] China Mobile USA planned to provide a variety of international services, including international interexchange services, international private line circuits, and mobile virtual network operator services, as well as data center and cloud services, for which no

---

[255] *Id.; In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, n.12 (May 10, 2019); *China Mobile Closing Down 3G System, Complete Switch-Off Expected by 2020*, TELEGEOGRAPHY (Mar. 11, 2019), https://www.telegeography.com/products/commsupdate/articles/2019/03/11/china-mobileclosing-down-3g-system-complete-switch-off-expected-by-2020/; *The World's Top 10 Telecommunications Companies*, INVESTOPEDIA (May 16, 2019), https://www.investopedia.com/articles/markets/030216/worlds-top-10-telecommunications-companies.asp.

[256] *See* CHINA MOBILE FY2019 FORM 20-F, *supra* note 123, at 21; *Investor Relations – Monthly Customer Data*, CHINA MOBILE LIMITED, https://www.chinamobileltd.com/en/ir/operation_m.php.

[257] *Investor Relations – Key Operation Data*, CHINA MOBILE LIMITED, https://www.chinamobileltd.com/en/ir/operation_y.php?scroll2title=1. *See* CHINA MOBILE FY2019 FORM 20-F, *supra* note 123, at 3.

[258] Application of China Mobile International (USA) Inc. for International Section 214 Authority, File No. ITC-214-20110901-00289, Attach. 2 (filed Sept. 1, 2011), https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=95289&acct=235487&id_form_num=2&filing_key=-233159; Amendment to Application of China Mobile International (USA) Inc. for International Section 214 Authority, File No. ITC-214-20110901-00289 (Jan. 30, 2015), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-233159&f_number=ITC2142011090100289.

[259] *See History – About Us*, CHINA MOBILE INTERNATIONAL, https://www.cmi.chinamobile.com/en/about/cmi; *Global Resources – Global Footprint*, CHINA MOBILE INTERNATIONAL, https://www.cmi.chinamobile.com/en/global-resources.

[260] *See Int'l Bureau Selected Applications Listing, File No. ITC-214-20110901-00289*, FED. COMMC'NS COMM'N, http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITC2142011090100289&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number (listing "date filed" as September 1, 2011); Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Report No. TEL-01519S (Sept. 16, 2011); *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3367, ¶ 4 (May 10, 2019).

Section 214 authorization is needed.[261] Team Telecom undertook a seven year review before ultimately recommending that the FCC deny the application on national security grounds. The FCC denied the application, but it did so nearly a year after receiving Team Telecom's recommendation.

1. Team Telecom's Review of China Mobile USA's Application Lasted Seven Years

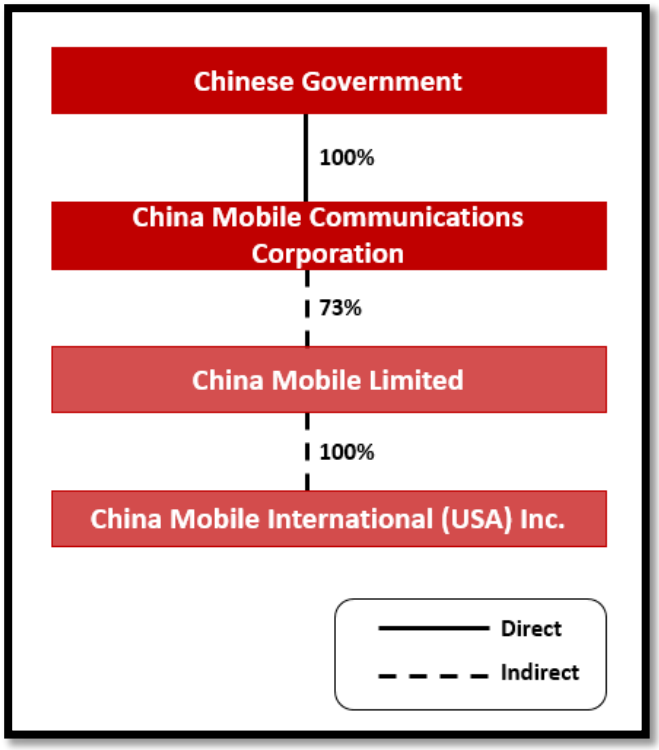
As noted above, China Mobile USA applied for Section 214 authorization on September 1, 2011.[262] The FCC referred the application to Team Telecom for its input on the national security and law enforcement risks posed by the proposed operations.[263] Team Telecom requested the application be removed from streamlining to give it additional time to evaluate concerns.[264] Team Telecom spent the next seven years evaluating the application, during which Team Telecom engaged China Mobile USA to "learn more about its management, business, and proposed activities."[265] China Mobile USA responded to Team Telecom's questions between 2011 and 2012 and again to another set of inquiries in 2014.[266] Not until July 2018, however, did Team Telecom—through the National Telecommunications and Information Administration ("NTIA")[267]—recommend that the FCC deny China Mobile USA's application. Team Telecom concluded that China Mobile USA's proposed services raised serious national security concerns that could not be sufficiently mitigated through a security agreement.[268] Team Telecom's concerns generally fell into the following categories.

China Mobile USA is ultimately owned by the Chinese government. Team Telecom noted that China Mobile USA, through intermediary companies, is majority owned and controlled by the Chinese government.[269] China Mobile USA is

---

[261] *See* Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Report No. TEL-01519S (Sept. 16, 2011); *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3367, ¶ 4 (May 10, 2019). *See also* Letter from J. Kostyu, Counsel to China Mobile International (USA) Inc., to Marlene Dortch, Sec'y, Fed. Commc'ns Comm'n (Mar. 12, 2013).
[262] *See In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3367, ¶ 4 (May 10, 2019).
[263] *Id.* at ¶ 5. Other Executive Branch agencies were also asked to opine on foreign policy and trade risks. *Id.*
[264] *Cf. id.*
[265] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 4.
[266] *Id.* at 4–5.
[267] Team Telecom works closely with other Executive Branch agencies to prepare a single recommendation on behalf of the Executive Branch. NTIA is responsible for filing that recommendation with the FCC. Briefing with the Dep't of Justice (Aug. 1, 2019). NTIA is a part of the Department of Commerce. *See About NTIA*, NAT'L TELECOMMC'NS & INFO. ADMIN., https://www.ntia.doc.gov/about.
[268] *Id.*; Li Tao, *Why the US Government Sees China Mobile as a National Security Threat*, SOUTH CHINA MORNING POST (July 4, 2018).
[269] *See In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3367 ¶ 19 (May 10, 2019).

a wholly-owned subsidiary of China Mobile. Although listed on both the New York and Hong Kong stock exchanges, China Mobile is majority owned by China Mobile Communications Corporation, "a Chinese state-owned enterprise subject to supervision of . . . [the State-owned Assets Supervision and Administration Commission ('SASAC')]."[270] "The Chinese government holds a direct 100 percent ownership interest in China Mobile Communications Corporation."[271] At the time China Mobile USA applied for Section 214 authorization, China Mobile Communications Corporation owned more than 70 percent of China Mobile.[272]



[273]

[270] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3. *See also* Application of China Mobile International (USA) Inc. for Authority to Provide International Facilities-Based and Resold Services to All International Points, at Attach. 2 – Answer to Question 14. In January 2015, China Mobile (USA) alerted the FCC that its immediate parent company had been transferred to China Mobile International (UK) Limited, which was also majority controlled by China Mobile Communications Corporation. Thus, the change was in name only and had no effect on China Mobile USA's ultimate ownership or its status as a Chinese state-owned entity. *See* Letter from K. Bressie et al., Counsel to China Mobile USA, to Marlene Dortch, Sec'y, Fed. Commc'ns Comm'n (Jan. 30, 2015).

[271] *See* Application of China Mobile International (USA) Inc. for Authority to Provide International Facilities-Based and Resold Services to All International Points, at Attach. 2 – Answer to Question 14.

[272] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3.

[273] The diagram is derived from information contained in *Executive Branch Recommendation re China Mobile USA*, *supra* note 56; *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361 (May 10, 2019); CHINA MOBILE FY2019 FORM 20-F, *supra* note 123.

China Mobile USA is vulnerable to exploitation, influence, and control by the Chinese government. Team Telecom concluded that China Mobile USA is vulnerable to exploitation, influence, and control by the Chinese government, in part because of its government ownership.[274] Team Telecom also noted that China Mobile USA would be required to comply with intercept requests from the Chinese government.[275]

China Mobile USA's authorization would allow it to interconnect with U.S. telecommunications networks and carriers. Team Telecom warned that, with Section 214 authorization, China Mobile USA would have been able "to interconnect [its international voice traffic] with the U.S. telecommunications network."[276] "A carrier connected to [the U.S. telecommunications networks] has greater access to telephone lines, fiber-optic cables, cellular networks, and communication satellites . . . ."[277] Further, China Mobile USA would have been able to build "direct and indirect interconnection relationships with other telecommunications carriers, from basic connections between networks in order to exchange traffic . . . to much more integrated relationships."[278] Access to these networks and relationships with U.S. carriers would provide China Mobile USA—and by extension the Chinese government—with access to critical infrastructure, which the Chinese government could use to further its espionage and intelligence activities.[279]

China Mobile USA's authorization would allow it to increase its operations in the United States without further FCC approval. The concern about China Mobile USA's access to the U.S. telecommunications networks was "amplified" given that,

> after obtaining an international Section 214 authorization, China Mobile [USA] could further expand its U.S. operations by increasing the number of its points of presence in the United States, developing its own domestic network without relying on underlying carriers for connectivity, increasing its number of peering partners, providing mobile service, or operating as a mobile virtual network operator.[280]

---

[274] *See Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 7–17. *See also In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, ¶¶ 8, 19 (May 10, 2019).

[275] *See Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 8. The Executive Branch also expressed concern that "there is a substantial risk that the Chinese government would exert even greater control over China Mobile and China Mobile USA than other state-owned enterprises given the Chinese government's 100% ownership of China Mobile, the size and reach of China Mobile and its subsidiaries, and the importance of any opportunities afforded by the telecommunications services offered both within China and globally." *See Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 8. *See also In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361 ¶¶ 8, 19 (May 10, 2019).

[276] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3.

[277] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 10.

[278] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3.

[279] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 3, 10.

[280] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 10–11.

Team Telecom warned that this contributed to a "substantial and unacceptable risk of increased economic espionage" against the United States.[281]

The Chinese government could use the grant of authority to China Mobile USA to further its cyber and economic espionage efforts against the United States. Team Telecom repeatedly warned that the Chinese government could use the grant of authority to China Mobile USA to further its espionage efforts against the United States.[282] Further, China Mobile USA could, at the request of the Chinese government, violate any security agreement with Team Telecom, as it may be required to do under Chinese law.[283] Even if breaches were reported and resolved, "the potential harms could very likely not be remediated."[284] Finally, Team Telecom concluded that it would be unable to work effectively with China Mobile USA or its parent companies to identify and disrupt unlawful activities, or to assist in the investigation of past and current unlawful conduct.[285]

2. Ten Months after Team Telecom's Recommendation, the FCC Denied China Mobile USA's Application on National Security Grounds

In May 2019—nearly a year after Team Telecom's July 2018 recommendation—the FCC voted unanimously to deny China Mobile USA's application.[286] The FCC accepted Team Telecom's national security rationale, explaining:

> [D]ue to a number of factors related to China Mobile USA's ownership and control by the Chinese government, grant of the application would raise substantial and serious national security and law enforcement risks that cannot be addressed through a [security] agreement.

---

[281] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 11.
[282] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 9–17.
[283] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 7.
[284] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56, at 16–17.
[285] *Executive Branch Recommendation re China Mobile USA*, *supra* note 56.
[286] *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3361, ¶ 1 (May 10, 2019); Press Release, Fed. Commc'ns Comm'n, FCC Denies China Mobile USA Application to Provide Telecommunications Services (May 9, 2019), https://docs.fcc.gov/public/attachments/DOC-357372A1.pdf. As noted above, during this time, China Mobile USA filed a reply to Team Telecom's recommendation and NTIA, on behalf of Team Telecom and the other Executive Branch agencies, filed a reply. *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3361, ¶ 1 (May 10, 2019). The FCC noted that staff "actively worked on the recommendation to deny from July 2018, when it was received" until the May 2019 order. It also suggested that it took longer to reach a decision because the "denial of an international Section 214 application on national security grounds was a case of first impression." *See* Email from the Fed. Commc'ns Comm'n to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

> Therefore, grant of [the] application would not be in the public interest.[287]

The FCC agreed that China Mobile USA was vulnerable to "exploitation, influence, and control by the Chinese government" and that there was a significant risk that the Chinese government would use the Section 214 authorization to further its economic and cyber espionage efforts against the United States.[288]

B. China Telecom Corporation and China Telecom Americas

China Telecom Corporation ("China Telecom"), a Chinese company and one of the Big Three providers in China, is an integrated information technology ("IT") services company that provides wireline, mobile telecommunications, Internet access, information and other telecommunications services.[289] It served more than 335 million subscribers worldwide as of December 31, 2019 and claims to be the largest fixed line and broadband operator in the world.[290]

China Telecom has been operating in the United States for nearly 20 years through its U.S. subsidiary, China Telecom Americas ("CTA"), a Delaware corporation.[291] CTA was founded in 2001 and obtained Section 214 authorization in 2002.[292] According to its website, CTA provides "a comprehensive range of high quality telecommunications services"[293] with the mission of delivering "high-quality data and voice solutions and services between the Americas and China to businesses and carriers."[294]

Team Telecom recently recommended the FCC revoke and terminate CTA's Section 214 authorizations. Although Team Telecom has recently begun exercising

---

[287] *In the Matter of China Mobile Int'l (USA) Inc.*, FCC No. 19-38, 34 FCC Rcd 3361, 3361, ¶ 1 (May 10, 2019).
[288] *Id.* at ¶¶ 8, 14–19, 30–33.
[289] *Overview*, CHINA TELECOM, https://www.chinatelecom-h.com/en/company/company_overview.php.
[290] *See* CHINA TELECOM FY2019 FORM 20-F, *supra* note 96, at 23; *Company Overview*, CHINA TELECOM AMERICAS, https://www.ctamericas.com/company/company-overview/.
[291] *See* CHINA TELECOM FY2019 FORM 20-F, *supra* note 96, at F-64. The company was originally named China Telecom USA, but changed its name to China Telecom Americas in October 2007 due to the company's expansion into Canada and Latin America. *See FAQ's*, CHINA TELECOM AMERICAS, https://www.ctamericas.com/faqs/.
[292] *See* CHINA TELECOM FY2019 FORM 20-F, *supra* note 96, at F-64; Briefing with Morgan, Lewis & Bockius LLP, counsel to CTA (May 7, 2020).
[293] *Global Network*, CHINA TELECOM AMERICAS, https://www.ctamericas.com/company/global-network/. CTA informed the Subcommittee that it does not provide all services listed on its website in the United States. Its U.S. services are limited to "data/connectivity services between the Americas, China, and primarily Asia and Mobile Virtual Network Operator ('MVNO') services via the CTExcel brand name." Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[294] *Company Overview – Mission*, CHINA TELECOM AMERICAS, https://www.ctamericas.com/company/company-overview/.

oversight of CTA's operations in the United States, it comes after years of minimal activity. When China Telecom applied for Section 214 authorization in 2001[295] and CTA separately applied for Section 214 authorization in 2002,[296] Team Telecom did not object or raise concerns about either's proposed services. Not until 2007 did Team Telecom enter into a security agreement with the company.[297] Since entering the security agreement, Team Telecom conducted just two site visits in 13 years.[298]

The lack of oversight and monitoring is concerning given that it occurred at a time when China Telecom and CTA were publicly alleged to have hijacked and rerouted data through China.[299] The incidents allegedly affected customers across major carriers, including Qwest Communications, Level 3 Communications, AT&T, and Verizon, and impacted both civilian and U.S. government customers.[300] The reported incidents involving CTA stretch back to 2010. Team Telecom, however, did not raise these issues with CTA until 2019.

1. The FCC Streamlined and Approved China Telecom's and CTA's Initial Section 214 Authorizations within Two Weeks

China Telecom applied for international Section 214 authorization in June 2001, before the establishment of CTA.[301] China Telecom sought to provide "facilities-based and resale services between the [United States] and permissible international points, *except China*."[302] Although the FCC referred the application to Team Telecom,[303] neither the FCC nor Team Telecom had records demonstrating that Team Telecom reviewed the application. Because Team Telecom did not object to the application, the FCC streamlined the application and approved it two weeks

---

[295] Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00417S, at 2 (July 6, 2001).
[296] Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00558S, at 2 (Aug. 7, 2002).
[297] Letter from Yi-jun Tan, President, China Telecom (USA) Corp., to Sigal Mandelker, Deputy Assistant Att'y Gen., Dep't of Justice, Elaine Lammert, Deputy Gen. Counsel, Fed. Bureau of Investigation, & Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec. (July 17, 2007).
[298] CTA informed the Subcommittee that, in recent years, it has interacted with Team Telecom on as many as 90 occasions. Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee). The majority of these occasions were through written correspondence.
[299] *See, e.g.*, Toonk, *supra* note 121; Madory, *supra* note 121; Shavitt & Demchak, *supra* note 109.
[300] *See, e.g.*, Toonk, *supra* note 121; Madory, *supra* note 121; Diaz, *supra* note 121.
[301] *See Int'l Bureau Selected Applications Listing, File No. ITC-214-20010613-00346*, FED. COMMC'NS COMM'N, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITC214200106130034 6&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number; FCC-PSI-000019–20; Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00417S, at 2 (July 6, 2001).
[302] *See* FCC-PSI-000019–20 (emphasis added); Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00417S, at 2 (July 6, 2001) (emphasis added).
[303] *See* FCC-PSI-000019–20.

after accepting it for filing.[304] In June 2002, after establishing CTA, China Telecom assigned its Section 214 authorization to its American subsidiary.[305]

The 2001 authorization limited CTA to providing international services between the United States and international points, other than China.[306] A month after receiving the authorization from China Telecom, CTA separately applied for international Section 214 authorization to serve as a facilities-based carrier between the United States and China.[307] Again, the FCC sought Team Telecom's input on the application, directly stating that CTA was "100% owned by [a People's Republic of China] state-owned entity . . . ."[308] As with the 2001 application, neither the FCC nor Team Telecom had records of Team Telecom responding to the FCC's request. The FCC streamlined and approved CTA's application within two weeks of accepting the application for filing.[309]

2. After a Change in Ownership in 2007, Team Telecom Sought a Security Agreement with CTA

Team Telecom did not interact with CTA between 2002 and 2007. In fact, documents suggest that Team Telecom may not have understood that, prior to 2007, CTA was providing services between the United States and China.[310] In 2007,

---

[304] *Compare* Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00417S, at 2 (July 6, 2001) *with* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00423, DA No. 01-1794, 16 FCC Rcd 14695, 14696 (July 26, 2001) (listing the authorization "date of action" as July 20, 2001—14 days after the public notice of acceptance of filing).

[305] *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00576, DA No. 02-2234, 17 FCC Rcd 16825, 16829 (Sept. 12, 2002) (listing the consummation date of the transfer as June 7, 2002).

[306] *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00423, DA No. 01-1794, 16 FCC Rcd 14695, 14696 (July 26, 2001). The authorization specifically noted that China Telecom was "prohibited from using its authorized U.S. international facilities or services to provide direct or indirect service to or from China unless and until it secures additional specific authority for such service . . . ." *See id.*

[307] *See* Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00558S, at 2 (Aug. 7, 2002).

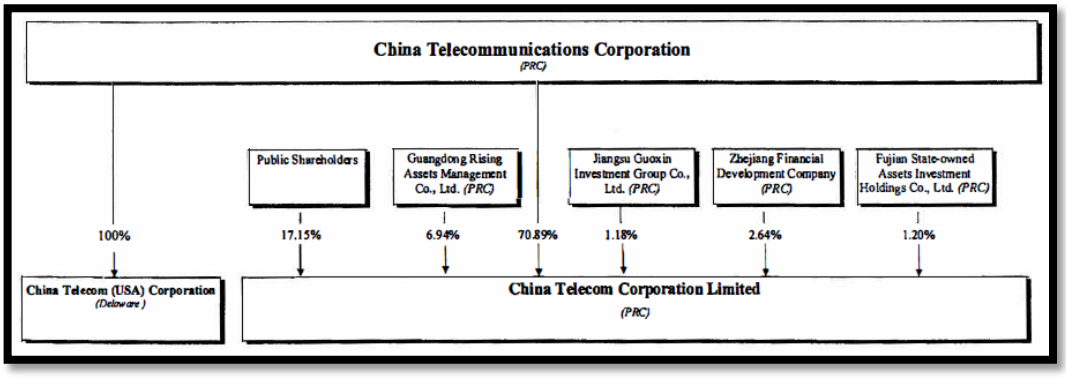
[308] FCC-PSI-000040–41.

[309] *Compare* Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00558S, at 2 (Aug. 7, 2002) *with* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00567, DA 02-2060, 17 FCC Rcd 16199, 16201 (Aug. 22, 2002) (listing the authorization "date of action" as August 21, 2002—14 days after accepting the application for filing).

[310] Team Telecom's report detailing its March 2017 site visit states, "CTA was established in the U.S. in 2002 with the transfer to CTA of an FCC Section 214 license originally issued to China Telecommunications Corporation. In 2007, CTA applied for FCC authorization to modify the 2002 license to provide direct data service between the U.S. and China for the first time. This service was explicitly prohibited under the 2002 license. The request was approved in 2007 . . . ." *See* DHS00473PSI. This, however, misstates the distinction between China Telecom's June 2002 transfer of its Section 214 authorization to CTA and CTA's separate Section 214 authorization,

China Telecom restructured its operations, with China Telecom Corporation Limited ("CTCL")—also a Chinese company—acquiring full equity interest in CTA from China Telecom.[311] The stated purpose of the ownership change was for China Telecom to "structure its business and operations in an efficient manner."[312] But, the change had no impact on CTA's ultimate ownership.[313]

Pre-Transaction Structure



[314]

granted in August 2002. *See supra* Part IV.B.1. Team Telecom officials informed the Subcommittee that they were aware of CTA's August 2002 authorization and the 2002 license described in the March 2017 site visit report refers to CTA's August 2002 authorization. *See* Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee). As evidenced above, however, the report only references the authorization China Telecom transferred to CTA; it makes no reference to CTA's August 2002 authorization.

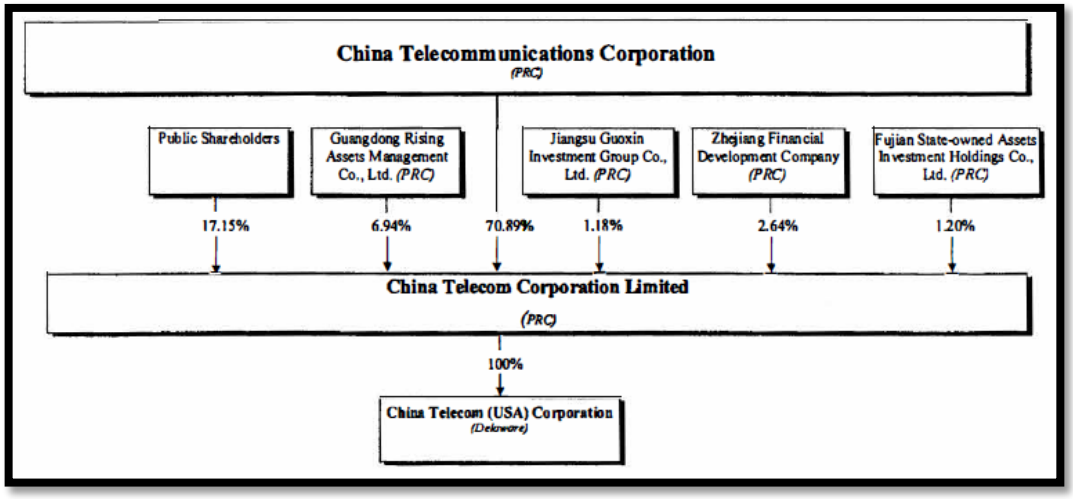
[311] China Telecom (USA) Corp. Application for International Section 214 Authorization for Assignment or Transfer of Control, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=69776&acct=434900&id_form_num=17&filing_key=-133273.

[312] *Id.* at Attach. 1.

[313] *Id.* According to Team Telecom's records, CTA informed Team Telecom that China Telecom had the ability to control the election of CTCL's directors; approve CTCL's budget; approve mergers and acquisitions; amend the Articles of Association; determine the timing and amount of dividend payments; and determine the issuance of new securities. *See* TT-DOJ-001–10, at TT-DOJ-003. In discussions with the Subcommittee, CTA stressed that CTCL and China Telecom both have their own corporate governance safeguards and transparency controls. Further, as a publicly listed company, CTCL is "subject to rigorous legal regulation and public oversight." CTA told the Subcommittee that CTCL has a board of directors and senior management to run the company independently, with SASAC acting only as a capital contributor. Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

[314] *See* TT-DOJ-001–10, at TT-DOJ-012.

Post-Transaction Structure



315

As required under FCC regulations, CTA notified the FCC of the change in ownership on July 25, 2007.[316] The notification stated that CTA had "conferred with the Executive Branch with respect to the [change of ownership] transaction" and "[b]y letter dated July 17, 2007 to the U.S. Department of Justice, the Federal Bureau of Investigation, and the U.S. Department of Homeland Security, [CTA had] agreed to abide by certain commitments and undertakings."[317] According to current officials, Team Telecom learned of CTA's change in ownership through the FCC's public notice of the change and then decided to engage the company to assess potential national security risks.[318]

Around May 2007, Team Telecom sent CTA written inquiries regarding the types of services CTA was then providing in the United States and those it

---

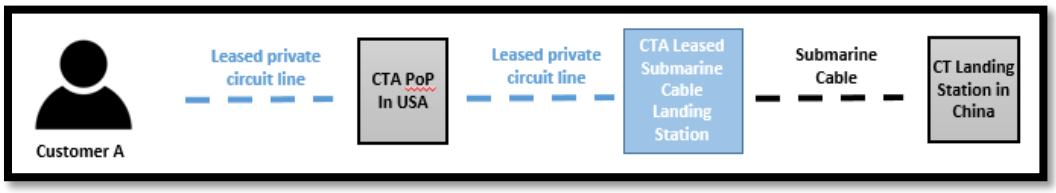
[315] *See id.* at TT-DOJ-013.

[316] *See* China Telecom (USA) Corp. Application for International Section 214 Authorization for Assignment or Transfer of Control, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITCT/C2007072500285&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number. The pro forma notice itself is not dated; however, an attachment to the notice indicates that the transfer of control occurred on July 12, 2007. The FCC's International Bureau Application database provides a filed date of July 25, 2007. *See Int'l Bureau Selected Applications Listing, File No. ITC-T/C-20070725-00285*, FED. COMMC'NS COMM'N, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITCT/C2007072500285&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number.

[317] China Telecom (USA) Corp. Notification of International Section 214 Authorization Assignment or Transfer of Control, at Attach. 1, p.4, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=69776&acct=434900&id_form_num=17&filing_key=-133273.

[318] *See* Briefing with the Dep't of Justice (Aug. 1, 2019). However, the pro forma notice and the FCC's application database suggest that the pro forma notice was not filed—at least publicly—until July 2007. *See supra* note 316.

anticipated providing in the future.[319] CTA informed Team Telecom that it was providing and anticipated continuing to provide international voice and data services, including wholesale voice traffic, private line, internet protocol ("IP"), and virtual private network ("VPN") services to China, Asia, and other international locations.[320] Notably, CTA stated that it did not market domestic U.S. voice or data services; rather, it was focused on international data services.[321] To transmit data internationally, CTA indicated that it maintained switches and routers in various U.S. cities and from these locations connected to U.S. carrier networks.[322] CTA "[took] traffic that is delivered to [its points of presence in the United States] through leased private circuits to [CTA's leased] submarine cable landing stations . . . where the traffic is routed to China and other foreign destinations."[323]



[324]

CTA's responses also indicated that, as of May 2007, its customers were split among enterprise customers and other telecommunications carriers throughout the United States.[325] While CTA stated that it had no government customers, it did note that it was a subcontractor to Qwest (subsequently acquired by CenturyLink) to provide services to the U.S. Embassy in Mongolia.[326] CTA told the Subcommittee that it ceased subcontracting with Qwest to serve the U.S. Embassy in Mongolia in 2012, and that, as of May 2020, it does not serve as a subcontractor to any entity that provides services to a U.S. governmental facility.[327]

---

[319] *See* TT-DOJ-001–10. The Department of Justice was unable to locate the correspondence in which it transmitted questions to China Telecom Americas.
[320] *See id.* at TT-DOJ-001.
[321] *Id.*
[322] *Id.* at TT-DOJ-006.
[323] *Id. See also* DHS00475PSI ("CTA does not provide last mile service to customers in the U.S., nor does it operate its own transmission infrastructure within the U.S. Instead, CTA uses its U.S. points of presence in major U.S. cities to aggregate customer data traffic for transmission across Tier 1 U.S. networks to its software switch with access to the Los Angeles endpoint of a trans-Pacific consortium submarine cable.").
[324] The diagram is derived from information contained at TT-DOJ-001–10.
[325] TT-DOJ-001–10, at TT-DOJ-001.
[326] *Id.* at TT-DOJ-002.
[327] Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee); Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (May 22, 2020) (on file with the Subcommittee).

In the May 2007 submission, CTA provided Team Telecom with a list of its top three executives—all of whom were Chinese nationals.[328] The only American CTA mentioned was its external legal counsel, who it also designated as the point of contact for law enforcement officials.[329] CTA indicated that all U.S. business records are stored in the United States and agreed to alert Team Telecom prior to storing such records abroad.[330]

Based on these responses, Team Telecom determined that security measures were warranted before it agreed to recommend that the FCC maintain CTA's Section 214 authorizations despite the change in ownership.[331] The parties negotiated a three-page security agreement.[332] Among other commitments, CTA agreed to (1) make U.S. customer records available in the United States in response to lawful U.S. process; (2) ensure that U.S. records are not made subject to mandatory destruction under foreign laws; (3) take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. records; (4) maintain one or more points of contact within the United States with the authority and responsibility for accepting and overseeing compliance with a lawful demand by U.S. law enforcement authorities; and (5) notify the FBI, DOJ, and DHS of any material changes in any of the facts in the security agreement or if it undertakes any action that requires notice or application to the FCC.[333]

On August 9, 2007, after executing the agreement, Team Telecom informed the FCC that it "ha[d] no objection to the [FCC] granting its consent [to the pro forma change of control], provided that the [FCC] condition[ed] the grant on [CTA] abiding by the commitments and undertakings contained in its July 17, 2007 letter to [Team Telecom]."[334] The FCC approved transfer of control on August 15, 2007,

---

[328] TT-DOJ-001–10, at TT-DOJ-003–04.
[329] *Id.* at TT-DOJ-004.
[330] *Id.* at TT-DOJ-005.
[331] *See, e.g.*, In the Matter of China Telecom (USA) Corporation – *Pro Forma* Transfer of Control from China Telecommunications Corporation to China Telecom Corporation Limited (File No. ITC-2014-20010613-00346; ITC-214-20020716-00371) – Petition to Adopt Conditions to Authorizations and Licenses (dated Aug. 9, 2007), https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=69776&acct=434900&id_form_num=17&filing_key=-133273; Letter from Yi-jun Tan, President, China Telecom (USA) Corp., to Sigal Mandelker, Deputy Assistant Att'y Gen., Dep't of Justice, Elaine Lammert, Deputy Gen. Counsel, Fed. Bureau of Investigation, & Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec. (July 17, 2007).
[332] *See* Letter from Yi-jun Tan, President, China Telecom (USA) Corp., to Sigal Mandelker, Deputy Assistant Att'y Gen., Dep't of Justice, Elaine Lammert, Deputy Gen. Counsel, Fed. Bureau of Investigation, & Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec. (July 17, 2007).
[333] *Id.*
[334] *See* In the Matter of China Telecom (USA) Corporation – *Pro Forma* Transfer of Control from China Telecommunications Corporation to China Telecom Corporation Limited (File No. ITC-2014-20010613-00346; ITC-214-20020716-00371) – Petition to Adopt Conditions to Authorizations and Licenses (dated Aug. 9, 2007), https://licensing.fcc.gov/cgi-

conditioned on CTA abiding by the commitments and undertakings contained in the July 2007 security agreement.[335]

3. Team Telecom's Oversight of CTA Since 2007 Has Consisted of Two Site Visits and Intermittent Email Communication

Team Telecom had limited engagement with CTA for nearly a decade after entering into the security agreement. Between 2007 and 2016, Team Telecom's oversight was limited to written correspondence in which CTA informed Team Telecom of changes to the company's law enforcement point of contact, among other information.[336] Documents provided to the Subcommittee by DOJ mention a meeting with CTA, the FCC, and Team Telecom sometime in 2014, during which CTA briefed the government officials on an anticipated China Telecom corporate restructuring.[337] Neither the FCC nor Team Telecom, however, could locate any contemporaneous records detailing the meeting.

When asked to explain the lack of oversight during this period, despite the security agreement being in effect, Team Telecom officials pointed to the security agreement, noting that because it was broadly written, demonstrating compliance was straightforward.[338] Officials also pointed to Team Telecom's lack of a compliance process before 2010.[339] Further, one official noted that Team Telecom's understanding of the risks associated with China and its state-owned entities evolved over time.[340] Still, even after 2011, Team Telecom believed it should complete review of China Mobile USA's pending application, as those deliberations

---

bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=69776&acct=434900&id_form_num=17&filing_key=-133273.

[335] *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01179, DA 07-3632, 22 FCC Rcd 15266, 15268 (Aug. 16, 2007) (listing the authorization "date of action" as August 15, 2007).

[336] *See* TT-DOJ-155–59. In addition to updating its point of contact, in November 2016, CTA informed Team Telecom of a 2014 corporate reorganization, during which, for a brief period, records of U.S. persons were stored outside of the United States. CTA also informed Team Telecom that it launched mobile virtual network operator ("MVNO") services under the brand name CTExcel in 2015; CTA resold T-Mobile services. *See* TT-DOJ-157–59.

[337] *See* TT-DOJ-157–59, at TT-DOJ-158.

[338] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).

[339] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

[340] *Id.*; Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee). The official referenced the House of Representatives Permanent Select Committee on Intelligence's 2012 Report on Huawei as evidence of the evolving understanding across the U.S. government. U.S. HOUSE OF REP. PERMANENT SELECT COMM. ON INTELLIGENCE, INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE (Oct. 8, 2012).

would be applicable to the existing authorizations of other Chinese state-owned carriers.[341]

Not until 2017 did Team Telecom begin to engage in substantive oversight of CTA. Team Telecom officials explained that, by this time, Team Telecom and the Executive Branch agencies were finalizing its recommendation to deny China Mobile USA's application.[342] Thus, it was a logical sequence to then assess Chinese state-owned carriers with existing authorizations.[343] This began with a site visit to CTA's Herndon, Virginia headquarters on March 10, 2017, during which Team Telecom officials spoke with company officials about its (1) corporate organization; (2) products and services; (3) telecommunications infrastructure; (4) data and voice networks; (5) data storage locations; and (6) law enforcement request and Commission on Accreditation for Law Enforcement Agencies ("CALEA") processes.[344] During that visit, CTA explained that its budget was subject to approval by China Telecom Global ("CTG")[345] and that CTG consulted on "technical matters that relate to the establishment of network points of presence . . . within the United States."[346] In fact, CTA noted that it established "a [new] Dallas [point of presence]" after "discussion" with CTG.[347] When asked, a current Team Telecom official described this as a traditional relationship between a state-owned enterprise and its subsidiary.[348] Although the official believed that CTA exists to conduct traditional and legitimate telecommunications business, he also noted that it was a Chinese state-owned entity and there is a latent risk that CTA's business interests may be overridden by geostrategic interests.[349]

During the 2017 site visit, Team Telecom also identified concerns related to CTA's storage of U.S. customer data.[350] Team Telecom records indicate that, for a period of time, CTA's records were stored in China; they were transferred back to

---

[341] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[342] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[343] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[344] *See generally* DHS00473PSI–76; TT-DOJ-495–99; TT-DOJ-500–06.
[345] In 2012, CTCL acquired China Telecom Global Limited, a Hong Kong company. *See* CHINA TELECOM CORP. LTD., ANNUAL REPORT (2016), https://www1.hkexnews.hk/listedco/listconews/sehk/2017/0406/ltn20170406631.pdf. China Telecom "streamlined its global business operations, establishing most operations outside China as divisions of [China Telecom Global]." TT-DOJ-495–99, at TT-DOJ-496.
[346] *See* DHS00473PSI–76, at DHS00473PSI; TT-DOJ-495–99, at TT-DOJ-497.
[347] *See* DHS00473PSI–76, at DHS00473PSI; TT-DOJ-495–99, at TT-DOJ-497.
[348] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).
[349] *Id.*
[350] Team Telecom defined "customer data" to include customer billing and service data, as well as sales information "such as name, address, billing information, and contract terms. For technical reasons, CTA also retains information about the location of customer data closets, paths to endpoints, and initial data connection points." TT-DOJ-495–99, at TT-DOJ-499.

the United States in 2014.[351] CTA also acknowledged that, "in 2015, CTA new customer information began to be ported onto a web-based platform located in China, with some existing customer data duplicated on this platform," although it eventually established a U.S-.based data storage system.[352] Team Telecom, however, noted that CTA passed certain customer data to CTG staff "at overseas network operations centers to manage enterprise data services . . ."[353] and that CTA "store[d] [U.S.] customer data in the [United States] and Hong Kong."[354] Team Telecom also flagged that CTA relied on China Telecom's network operations centers located in Beijing and Shanghai.[355] CTA informed the Subcommittee that customer information has always "remained available in the United States," with CTA being able to access the information.[356]

According to records of the site visit, one Team Telecom official concluded that CTA appeared to be "generally in compliance" with the security agreement, despite finding that CTA was not CALEA compliant and had "limited capability" of assisting law enforcement.[357] Officials acknowledged that Team Telecom needed to review CTA's equipment lists for potential security risks and, if needed, pursue modifications to the security agreement.[358] DHS indicated to the Subcommittee that DOJ—as the lead of Team Telecom—did not send a feedback letter to CTA following the March 2017 site visit to request the equipment list.[359] Nevertheless, one official explained that, even if such documents had been received and risks were identified, Team Telecom had limited recourse to force a renegotiation of the security agreement.[360]

Team Telecom conducted a second site visit in April 2018.[361] During that visit, CTA confirmed that it had no substantive or material changes since the 2017 visit, with the exception of elimination of wholesale voice services, which was deemed no longer profitable.[362] Handouts provided during the visit indicate CTA

---

[351] TT-DOJ-500–06, at TT-DOJ-502.
[352] TT-DOJ-495–99, at TT-DOJ-499.
[353] *Id.*; DHS00473PSI–76, at DHS00475PSI.
[354] TT-DOJ-500–06, at TT-DOJ-502.
[355] *Id.*
[356] Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[357] TT-DOJ-500–06, at TT-DOJ-502–03.
[358] *See* TT-DOJ-495–99, at TT-DOJ-496.
[359] *See* Email from the Dep't of Homeland Sec. to the Subcommittee (Feb. 14, 2020) (on file with the Subcommittee).
[360] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[361] *See generally* DHS00477PSI–99; TT-DOJ-507–20.
[362] DHS00477PSI–99, at DHS00478PSI; TT-DOJ-507–20, at TT-DOJ-508.

had points of presence in 11 U.S. cities, as well as eight data centers in four U.S. cities.[363]

Following the meeting, Team Telecom requested additional information about CTA's security policies and procedures, including whether Chinese security agencies had inspected or otherwise required information concerning CTA's operations.[364] Although CTA informed Team Telecom that no security agencies had inspected or required information gathering regarding CTA's operations, it did acknowledge that its procurement processes, including that of network equipment and software, are led by China Telecom.[365]

4. Team Telecom Did Not Engage CTA regarding Public Allegations that China Telecom and Its Affiliates Hijacked and Rerouted Data through China

As described above, hijacking communications is easier with the support of a complicit and preferably largescale carrier.[366] Public reports allege that China Telecom and its affiliates have hijacked and rerouted data through China on multiple occasions for more than a decade.[367] Nevertheless, Team Telecom did not address the allegations until early 2019.

a. Allegations of China Telecom Hijacking Communications Data Date Back to 2010

In April 2010, online reports alleged that China Telecom originated approximately 37,000 false routes in less than 20 minutes.[368] Customers of Telefonica, Qwest, Deutsche Telekom, Level 3 Communications, AT&T, and NTT allegedly had their communications hijacked and rerouted through China.[369] According to analysts, "China absorbed 15% of the traffic from U.S. military and civilian networks."[370] According to the U.S.-China Economic and Security Review Commission,

---

[363] TT-DOJ-507–20, at TT-DOJ-514–15. The points of presence were located in Palo Alto, CA; San Jose, CA; Los Angeles, CA; Hillsboro, OR; Denver, CO; New York, NY; Seattle, WA; Ashburn, VA; Miami, FL; Chicago, IL; and Dallas, TX. CTA also reported a point of presence in Toronto, Ontario, Canada. *See* TT-DOJ-514. CTA's data centers included four locations in Santa Clara, CA; one location each in Los Angeles, CA and Dallas, TX; and two locations in Ashburn, VA. *See* TT-DOJ-515.

[364] TT-DOJ-180–81.

[365] TT-DOJ-189–91.

[366] Shavitt & Demchak, *supra* note 109, at 3.

[367] *See, e.g.*, Shavitt & Demchak, *supra* note 109, at 3.

[368] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, REPORT TO CONGRESS 1, 243–44 (2010); Toonk, *supra* note 121.

[369] Toonk, *supra* note 121.

[370] Diaz, *supra* note 121. *See also* U.S.-CHINA ECONOMIC & SECURITY REVIEW COMMISSION, REPORT TO CONGRESS 244 (2010). *Cf.* Toonk, *supra* note 121.

> This incident affected traffic to and from U.S. government (".gov") and military (".mil") sites, including those for the Senate, the army, the navy, the marine corps, the air force, the office of secretary of Defense, the National Aeronautics and Space Administration, the Department of Commerce, the National Oceanic and Atmospheric Administration, and many others.[371]

The Commission also noted that the disruption could allow the carrier to "compromise the integrity of supposedly secure encrypted sessions."[372] There was no consensus, however, on the motives underlying the false routes. Some saw it as an unintentional error, while others concluded it was likely a "deliberated [*sic*] attempt to capture as much data as possible."[373]

Just a year later, new reports circulated about a similar incident in which AT&T and other U.S. carriers routed Facebook traffic through China.[374] The routing was allegedly the result of China Telecom advertising false routes for approximately nine hours.[375] Subsequent reports claimed that in December 2015, China Telecom hijacked traffic by advertising more than 300 false routes associated with Verizon's Asia Pacific ("APAC") region; the advertised routes were picked up by SK Broadband, a China Telecom transit partner.[376] SK Broadband then promoted those false routes to other carriers, including Telia, Tata, GTT, and Vodafone.[377] Networks around the world that accepted these routes inadvertently sent traffic to Verizon APAC through China Telecom.[378] Verizon informed the Subcommittee that its investigation into the alleged hijacking found no link to China Telecom, the Chinese government, or malicious activity.[379] Rather, it determined that the "hijack" was the result of human error by one of Verizon's peering partners.[380]

---

[371] U.S.-CHINA ECON. & SEC. REVIEW COMM'N, REPORT TO CONGRESS 1, 244 (2010).
[372] *Id.*
[373] *Compare* Toonk, *supra* note 121 (concluding that, given the short time frame and large number of announced routes, the hijack was likely the result of a configuration issue) *with* Diaz, *supra* note 121 ("Security expert Dmitri Alperovitch—VP of threat research at McAfee—says that this happens 'accidentally' a few times a year, but this time it was different: The China Telecom network absorbed all the data and returned it without any significant delay. Before, this kind of accident would have resulted in communication problems, which lead experts to believe this wasn't an accident but a deliberated attempt to capture as much data as possible.").
[374] Andree Toonk, *Facebook's detour through China and Korea*, BGPMON (Mar. 26, 2011), https://bgpmon.net/facebooks-detour-through-china-and-korea/.
[375] *Id.*
[376] Madory, *supra* note 121.
[377] Madory, *supra* note 121.
[378] Madory, *supra* note 121.
[379] Briefing with Verizon (Sept. 4, 2019).
[380] *Id.* The peering partner was not a Chinese carrier. *Id.*

More recently, a 2018 paper from researchers at the U.S. Naval War College and Tel Aviv University detailed a series of incidents between 2016 and 2017 in which the Chinese government allegedly used China Telecom to hijack telecommunications traffic.[381] The incidents outlined included diversion of (1) traffic from Canada that was intended for Korean government sites; (2) traffic from various U.S. locations directed to a large Anglo-American bank based in Milan; (3) traffic from Sweden and Norway intended for the Japanese network of a large American news organization; (4) traffic from a large Italian financial company to Thailand; and (5) traffic from providers in South Korea.[382] The Director of Oracle's Internet Analysis Division confirmed the researchers' findings, although he stopped short of addressing claims about the motivations underlying the hijacks.[383]

The authors of the 2018 paper noted that all of the incidents involved routing of the diverted communications to China through CTA's points of presence in the United States.[384] They explained that China Telecom was in a unique position to engage in this activity because it had "strategically placed, Chinese controlled internet points of presence across the internet backbone of North America."[385] One of the authors informed the Subcommittee that he believed China Telecom could not have carried out such hijacking attacks if it had not established operations within the United States.[386]

The events described above all occurred prior to Team Telecom's first site visit to CTA. Alleged incidents, however, continued after Team Telecom's site visits. For example, in November 2018, for over an hour, China Telecom allegedly erroneously advertised routes from a Nigerian ISP that resulted in traffic being routed through China.[387] "This incident at a minimum caused a massive denial of service to G Suite and Google Search. . . . Overall [analysts] detected over 180 prefixes affected by this route leak, which covers a vast scope of Google services."[388]

---

[381] Shavitt & Demchak, *supra* note 109.
[382] Shavitt & Demchak, *supra* note 109, at 5–7.
[383] Madory, *supra* note 121. In describing the allegations, Madory referred to the incidents as "misdirections." *See* Madory, *supra* note 121.
[384] *See* Shavitt & Demchak, *supra* note 109, at 5–7.
[385] *See generally* Shavitt & Demchak, *supra* note 109. As noted above, as of 2020, CTA purports to have points of presence in 13 cities across America. *See Global Data Center Ma*p, CHINA TELECOM AMERICAS, https://www .ctamericas.com/ global-data-center-map/.
[386] Briefing with BGProject (July 1, 2019).
[387] Ameet Naik, *Internet Vulnerability Takes Down Google*, THOUSAND EYES BLOG (Nov. 12, 2018), https://blog.thousandeyes.com/internet-vulnerability-takes-down-google/.
[388] *Id.* China Telecom denied hijacking the data. In a release, it noted that the company "promptly commenced a serious and thorough investigation . . . [which] found that the re-routing of Google data traffic stemmed from erroneous routing configuration by a Nigerian operator MainOne Cable . . . causing the Google data traffic, which was originally directed by MainOne Cable, to be mistakenly sent to China Telecom." The company also acknowledged that "it is normal for Americas or Europe data traffic to route through China Telecom's international network." Press Release, China Telecom Corp. Ltd., Statement Regarding the Unfounded Report on China Telecom Being

In connection with its recommendation to revoke CTA's Section 214 authorizations, Team Telecom noted that, despite CTA not being involved in the misdirection, the Nigerian-China Telecom error was "amplified" by China Telecom's presence in the United States, as it promoted false routes to U.S. carriers, thereby causing U.S. communications to be routed through China.[389]

When asked about these allegations, CTA explained to the Subcommittee that the allegations were "misleading" and "lack[ed] context about the reality of internet routing today."[390] CTA added that routing problems are common and occur on all networks, despite the best efforts of responsible operators.[391] Further, CTA maintained that "erroneous route information propagated to [China Telecom] by other networks was the cause of several [of the] incidents" referenced above and in Team Telecom's recommendation to revoke and terminate CTA's Section 214 authorizations.[392]

b. Despite Nearly a Decade of Allegations, Team Telecom Did Not Probe the Issue until January 2019

Allegations of hijacking involving China Telecom date back to 2010; however, Team Telecom did not question CTA about these reports until January 2019. Almost a year after its last site visit, Team Telecom sent written interrogatories to CTA, asking it to formally respond to the hijacking allegations, particularly those detailed in the 2018 paper from researchers at the U.S. Naval War College and Tel Aviv University.[393] CTA denied the allegations, arguing that it had never engaged in hijacking and had no incentive to do so.[394] CTA also noted that the public allegations contained no evidence of intentional or malicious wrongdoing.[395] As it did in conversations with the Subcommittee, CTA informed Team Telecom that certain of the public allegations were caused by other networks' erroneous route information that passed through China Telecom's networks.[396]

Team Telecom appears to have relied on CTA's written representations regarding the alleged incidents. Team Telecom provided no records or explanation of it conducting further interviews, requesting or reviewing additional documentation, or otherwise questioning CTA's assertions.

Alleged "Hijacking Internet Traffic" (Nov. 22, 2018), https://www.chinatelecom-h.com/en/media/news/p181122.php.

[389] *Executive Branch Recommendation re CTA*, *supra* note 56, at 49–50.

[390] Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

[391] *Id.*

[392] *Id.*

[393] TT-DOJ-264–69.

[394] *Id.*

[395] *Id.* *See also* Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

[396] TT-DOJ-264–69.

5. Nearly Two Decades after Obtaining Section 214 Authorization, Team Telecom Recommended CTA's Authorizations Be Revoked and Terminated

Nearly 20 years after CTA obtained Section 214 authorization, 13 years after entering into a security agreement, and two years after its last site visit, Team Telecom recommended the FCC revoke and terminate CTA's Section 214 authorizations because of "substantial and unacceptable" national security risks.[397] Team Telecom argued that the national security environment had changed significantly since 2007 and the national security concerns associated with CTA's operations could no longer be mitigated.[398] Team Telecom's arguments for revocation generally fell into the following categories.[399]

CTA's Section 214 authorization allows it to expand services without further FCC approval. Team Telecom explained that CTA uses its Section 214 authorizations to provide "regulated and unregulated services as a 'one-stop' provider of a 'full suite' of communications services."[400] Team Telecom warned that, with its facilities-based authorization, CTA does not require further FCC approval to expand its network or upgrade its equipment.[401] "The potential for [CTA] to increase its capabilities . . . heightens the national security and law enforcement concerns . . . ."[402]

CTA's Section 214 authorization allows it to build relationships with U.S. carriers. Team Telecom also warned that CTA's facilities-based authorizations allow it to request interconnections with U.S. carriers.[403] CTA has already established relationships with major U.S. carriers, including Verizon, CenturyLink,

---

[397] *Executive Branch Recommendation re CTA*, *supra* note 56. CTA told the Subcommittee that Team Telecom did not inquire whether CTA would be prepared to consider another security agreement prior to submitting its recommendation to the FCC. Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee). Team Telecom's recommendation, however, stated that Team Telecom felt further mitigation would be insufficient "because the underlying foundation of trust that is needed for a [security] agreement to adequately address national security and law enforcement concerns is not present." *Executive Branch Recommendation re CTA*, *supra* note 56, at 53.

[398] *Executive Branch Recommendation re CTA*, *supra* note 56, at 1–2.

[399] The information described below is based on Team Telecom's recommendation. CTA informed the Subcommittee that it disputes Team Telecom's allegations and "explicitly denies the assertions that it has engaged in intentional hijacking or that its licenses provide opportunities for China to engage in espionage against the United States." Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).

[400] *Executive Branch Recommendation re CTA*, *supra* note 56, at 8 (citing *General FAQs*, CHINA TELECOM AMERICAS, https://www.ctamericas.com/faqs). Team Telecom referenced CTA's provision of international private lines, mobile virtual network operator, MPLS VPN, SD-WAN, Ethernet, data center, and cloud services. *See Executive Branch Recommendation re CTA*, *supra* note 56, at 8–10.

[401] *Executive Branch Recommendation re CTA*, *supra* note 56, at 11–12.

[402] *Executive Branch Recommendation re CTA*, *supra* note 56, at 12.

[403] *Executive Branch Recommendation re CTA*, *supra* note 56, at 11–12.

and AT&T.[404] These relationships primarily include the provision of network or other retail services.[405] Verizon maintains an interconnection agreement and peering arrangement with CTA, as well as separate agreements with its Chinese parent companies.[406] Although CenturyLink does not maintain any formal partnership or arrangement with CTA, it does have a limited commercial relationship with the company.[407] CenturyLink did not specify the nature of its commercial relationship with CTA; rather, it generally described the relationship as involving the sale of network services, circuits, or collocation services.[408] These services allow CTA to deliver traffic from a CTA point of presence through CenturyLink's network to a CTA customer located in the United States.[409]

AT&T sells CTA voice and data transport services, which CTA uses to provide services to its customers in the United States.[410] AT&T has also established relationships with China Telecom. The two companies maintain a free-of-charge peering arrangement.[411] Further, the companies established a joint venture—Shanghai Symphony Telecommunications—in 2001.[412] While China Telecom is the majority stakeholder, AT&T owns a 25 percent stake in the venture.[413] The joint venture only provides services within the Pudong district of Shanghai; however, it has separately entered into contractual agreements with China Telecom, China Unicom, and China Mobile to provide VPN and other IP-based services throughout China.[414] The joint venture is set to expire in 2039.[415]

Neither Verizon, AT&T, nor CenturyLink maintains any mitigation or other agreement focused on network security with CTA or its parent company.[416] The

---

[404] Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019).
[405] Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019).
[406] Briefing with Verizon (Sept. 4, 2019).
[407] Briefing with CenturyLink (Sept. 10, 2019).
[408] *Id.*
[409] *Id.* CenturyLink purchases the same network services from Chinese carriers in China, to allow CenturyLink to deliver traffic to a CenturyLink customer based in China. *Id.*
[410] Briefing with AT&T (Sept. 17, 2019). AT&T representatives told the Subcommittee that the revenue generated by these agreements is relatively small, particularly when compared to similar agreements with other large international carriers. For example, similar arrangements with other large international carriers generate up to 36 to 62 times as much revenue as arrangements with the Chinese state-owned carriers discussed in this report. *Id.*; Email from Gibson, Dunn & Crutcher LLP, counsel to AT&T, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[411] Briefing with AT&T (Sept. 17, 2019). AT&T described the peering arrangement as "among the smallest . . . in terms of network capacity that AT&T maintains" with foreign carriers. *Id.*
[412] *Id.*
[413] *Id.*
[414] Teleconference with Gibson, Dunn & Crutcher LLP, counsel to AT&T (Oct. 15, 2019).
[415] Email from Gibson, Dunn & Crutcher LLP, counsel to AT&T, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[416] *See* Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019).

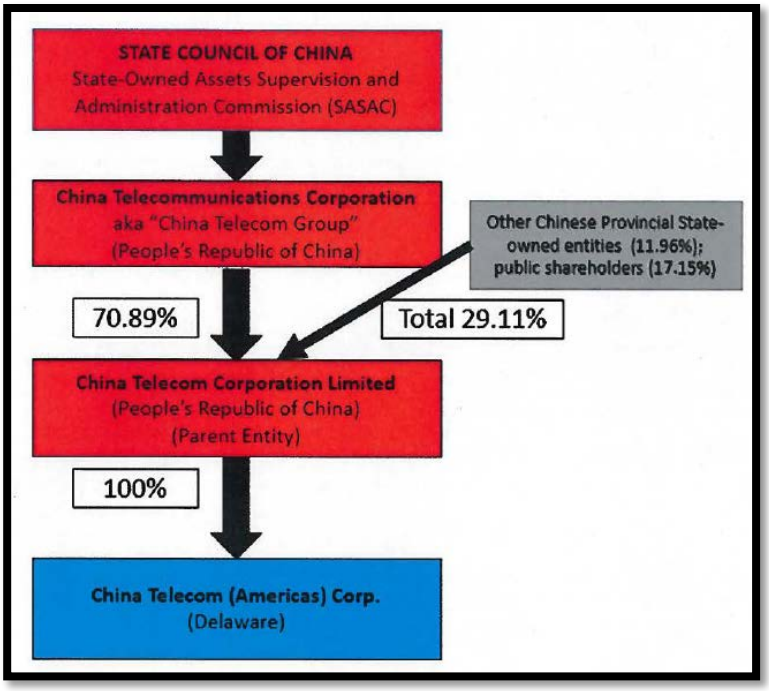
contractual service agreements with the Chinese state-owned carriers contain standard provisions indicating that the parties agree to deliver traffic to the intended recipient.[417] All three U.S. carriers, however, noted that they maintain company-wide cybersecurity defenses that apply to all external traffic, regardless of whether service or interconnection agreements exist.[418]

CTA is untrustworthy. Team Telecom highlighted CTA's delayed response to its document and information requests following the April 2018 site visit, which called into question CTA's willingness to comply with the security agreement.[419] When CTA finally produced the requested documents and information, Team Telecom identified what it viewed as prior inaccurate statements about where CTA stored its U.S. records.[420] Team Telecom also found that CTA's lack of trustworthiness negated the effectiveness of the security agreement and any further mitigation efforts.[421] Team Telecom added that CTA had breached the security agreement by failing to implement a formal written information security policy prior to December 1, 2018, and failing to notify Team Telecom of two 2010 FCC applications related to signaling point code.[422]

CTA is ultimately owned by the Chinese government. Team Telecom highlighted CTA's ownership structure and that CTA is ultimately owned and controlled, through CTCL and China Telecom, by SASAC:

---

[417] *See* Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019). Verizon representatives told the Subcommittee that Verizon's interconnection agreements with Chinese state-owned carriers are substantially identical to the agreements in place with other external carriers. Teleconference with Verizon (June 2, 2020).
[418] Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019); Teleconference with Verizon (June 2, 2020); Email from CenturyLink to the Subcommittee (June 2, 2020) (on file with the Subcommittee); Email from Gibson, Dunn & Crutcher LLP, counsel to AT&T, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[419] *Executive Branch Recommendation re CTA*, *supra* note 56, at 17.
[420] *Executive Branch Recommendation re CTA*, *supra* note 56, at 18–26. Team Telecom also believes CTA made inaccurate statements to U.S. customers about its cybersecurity practices. *Executive Branch Recommendation re CTA*, *supra* note 56, at 26–32.
[421] *Executive Branch Recommendation re CTA*, *supra* note 56, at 53–56.
[422] *Executive Branch Recommendation re CTA*, *supra* note 56, at 53–55. *See also* TT-DOJ-277–80. Signal point codes are unique addresses that identify individual network elements for a Signaling Point used in Message Transfer Part to identify the destination of a message signal unit. They operate similar to IP addresses. *See SS7 Point Code Administration*, ICONECTIV, https://iconectiv.com/ss7. In documents made available to the Subcommittee, CTA refuted the allegations, arguing that (1) the lack of a comprehensive information security policy was not indicative of a breach of obligations, and (2) the security agreement's obligations require CTA to alert Team Telecom only of actions that would result in a material change to the company's ownership structure, service offerings, or its ability to ensure the availability of its U.S. records in the United States. CTA argued that signal point codes do not fall into any of those categories. TT-DOJ-283–90.



[423]

Due to this ownership, Team Telecom warned that CTA "is vulnerable to exploitation, influence, and control by the Chinese government."[424] Team Telecom indicated that CTA will be forced to comply—and has complied—with Chinese government requests, including those made pursuant to China's recent cybersecurity and national security laws.[425]

In addition to its Chinese government ownership, CTA provides services to Chinese government facilities in the United States.[426]

CTA's U.S. operations provide opportunities for China to engage in economic espionage against the United States. Team Telecom reiterated warnings of other U.S. government officials concerning the Chinese government's cyber and economic espionage efforts against the United States.[427] Through its Section 214 authorizations, Team Telecom noted that CTA has greater "access to more customers, communications traffic, and interconnections with other U.S. common

[423] *Executive Branch Recommendation re CTA*, *supra* note 56, at 33.
[424] *Executive Branch Recommendation re CTA*, *supra* note 56, at 34.
[425] *Executive Branch Recommendation re CTA*, *supra* note 56, at 37–40. In discussions with the Subcommittee, CTA refuted Team Telecom's characterization that it has complied with Chinese government requests, describing it as "misleading and based on fear of some future hypothetical event, not substantiated by any proof of existing conduct." Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[426] Letter from Morgan, Lewis & Bockius LLP, counsel to CTA, to the Subcommittee (May 22, 2020) (on file with the Subcommittee).
[427] *Executive Branch Recommendation re CTA*, *supra* note 56, at 41–42.

carriers than it would have otherwise."[428] Team Telecom pointed specifically to CTA's managed service provider services, as well as China Telecom's ability to access CTA's U.S. customer records.[429] Team Telecom also highlighted allegations that China Telecom hijacked data on a number of occasions dating back to 2010.[430]

* * * * *

The FCC is currently considering Team Telecom's recommendation to revoke and terminate CTA's Section 214 authorizations. The FCC has ordered CTA to respond to Team Telecom's allegations and demonstrate why its Section 214 authorizations should not be revoked.[431] That order is currently pending; CTA is required to submit its response by June 8, 2020.[432]

C. China Unicom and China Unicom (Americas) Operations Limited

China United Network Communications Group Company Limited ("China Unicom") is considered the seventh largest mobile operator in the world based on number of subscribers.[433] According to its most recent 20-F filing with the SEC, China Unicom served approximately 318 million mobile subscribers worldwide as of December 31, 2019 and a reported revenue of nearly $42 billion.[434]

China Unicom's origins date back to 1994, when its predecessor company was founded by the Chinese government to compete with China Mobile, China's incumbent wireless provider.[435] In 2008, among other restructuring efforts, China Unicom's predecessor company merged with China Network Communications

[428] *Executive Branch Recommendation re CTA*, *supra* note 56, at 41.
[429] *Executive Branch Recommendation re CTA*, *supra* note 56, at 42–43.
[430] *Executive Branch Recommendation re CTA*, *supra* note 56, at 44–50.
[431] *See In the Matter of China Telecom (Americas) Corporation*, DA 20-448 (Apr. 24, 2020), https://docs.fcc.gov/public/attachments/DA-20-448A1.pdf.
[432] *See* Letter from Denise Coca, Chief, Telecommc'ns & Analysis Div., Int'l Bureau, Fed. Commc'ns Comm'n to Andrew Lipman, Counsel to CTA, Morgan, Lewis & Bockius LLP (May 14, 2020).
[433] The ranking is based on number of subscribers as of January 2019. *See* Abayomi Jegede, *Top 10 Largest Mobile Networks in the World by Subscribers*, THE DAILY RECORDS (Jan. 1, 2019), http://www.thedailyrecords.com/2018-2019-2020-2021/world-famous-top-10-list/highest-selling-brands-products-companies-reviews/best-largest-mobile-networks-world-by-subscribers-telecom-companies-revenue/12837/.
[434] CHINA UNICOM (HONG KONG) LTD. ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(D) OF THE SEC. EXCH. ACT OF 1934 FOR THE FISCAL YEAR ENDED DECEMBER 31, 2019 (FORM 20-F), COMM. FILE NO. 1-15028, at 2, 27 (filed Apr. 22, 2020), https://www.chinaunicom.com.hk/en/ir/reports/2019_20f.pdf [hereinafter CHINA UNICOM FY2019 FORM 20-F].
[435] Briefing with China Unicom Americas (Apr. 16, 2020).

Group Corporation ("China Netcom").[436] China Unicom was the resulting company.[437]

China Unicom (Americas) Operations Limited ("CUA") is China Unicom's American subsidiary and largest international affiliate.[438] CUA has operated in the United States since 2002, when it was granted its international Section 214 authorization.[439] Team Telecom, however, has never required CUA to enter into a security agreement, meaning it has not engaged CUA since its establishment.[440] Yet, CUA shares many characteristics with CTA and China Mobile USA, including government ownership, relationship to its parent entity, similar services and infrastructure across the United States, and partnerships with major U.S. carriers.[441]

1. The FCC Approved CUA's Section 214 Application in Two Weeks after Team Telecom Raised No Concerns

CUA applied for Section 214 authorization in July 2002 to provide facilities-based and resale services between the United States and all permissible international points, including China.[442] In mid-August 2002, consistent with its standard practice, the FCC asked Team Telecom to review the application for any

---

[436] CHINA UNICOM FY2019 FORM 20-F, *supra* note 434, at 21–22. The Chinese government established China Netcom in 1999 to serve as the incumbent wireline provider in Northern China. However, by 2008, the Chinese government determined that China Netcom was too small to enjoy a competitive advantage and merged it with China Unicom. Briefing with China Unicom Americas (Apr. 16, 2020).

[437] *Company Profile*, CHINA UNICOM GROUP, https://www.chinaunicomglobal.com/us/company. *See also* Briefing with China Unicom Americas (Apr. 16, 2020).

[438] Briefing with China Unicom Americas (Apr. 16, 2020).

[439] CUA was initially established under the name China Unicom USA LLC. It converted from an LLC to a corporation in 2003. The company's name was officially changed to CUA following China Unicom's merger with China Netcom. *See* Briefing with China Unicom Americas (Apr. 16, 2020); Letter from Squire Patton Boggs, counsel to CUA, to the Subcommittee (Apr. 29, 2020) (on file with the Subcommittee).

[440] Briefing with China Unicom Americas (Apr. 16, 2020); Briefing with the Dep't of Justice (Apr. 3, 2020); Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Briefing with the Dep't of Justice (Aug. 1, 2019).

[441] In discussions with the Subcommittee, CUA stressed that it also differs significantly from China Mobile USA and CTA with respect to shareholding structure, corporate governance, and history of compliance with the U.S. government. It further noted that there are many government-owned telecommunications carriers operating in the United States with operations and infrastructure similar to CUA. *See* Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).

[442] *See Int'l Bureau Selected Applications Listing, File No. ITC-214-20020724-00427*, FED. COMMC'NS COMM'N, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/swr031b.hts?q_set=V_SITE_ANTENNA_FREQ.file_numberC/File+Number/%3D/ITC2142002072400427&prepare=&column=V_SITE_ANTENNA_FREQ.file_numberC/File+Number (listing a filing date of July 24, 2002). As noted above, at the time of the application, the company was named China Unicom USA LLC. *See supra* note 439.

national security or law enforcement risks.[443] The FCC's referral noted that CUA's ultimate parent company was a state-owned enterprise.[444] The FCC asked that Team Telecom relay any concerns by September 3, 2002 "because [the FCC was] prepared to take action on the[ ] application[ ]."[445]

Neither the FCC nor Team Telecom had any record of Team Telecom raising concerns about the application. On September 13, 2002, the FCC issued a public notice formally accepting CUA's application for filing.[446] Because Team Telecom raised no concerns about the application, the FCC granted the application two weeks later.[447]

2. Team Telecom Has Never Engaged in Post-Authorization Oversight of CUA

Team Telecom never entered into a security agreement with CUA, despite CUA having filed pro forma notices with the FCC giving Team Telecom the opportunity to request such an agreement. For example, CUA filed notices in 2008 and 2009 regarding organizational changes associated with the Chinese government's restructuring of the Chinese telecom industry, China Unicom's merger with China Netcom, and changes to the company name.[448] More recently, in

---

[443] *See* FCC-PSI-000213–14.
[444] *See id.*
[445] *See id.*
[446] *See* Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00575S, at 2 (Sept. 13, 2002).
[447] *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00581, DA No. 02-2500, 17 FCC Rcd 19181, 19182 (Oct. 3, 2002) (listing the "date of action" authorizing the application as September 27, 2002 – 14 days after FCC's acceptance of filing public notice). China Netcom (USA) Operations Limited also applied for Section 214 authorization in 2002 to serve as a facilities based carrier. Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00568S, at 2 (Aug. 28, 2002). The FCC referred the application to Team Telecom, *see* FCC-PSI-000227–28, but Team Telecom never raised any concerns about the application. The FCC approved the application two weeks after accepting it for filing. *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00576, DA 02-2234, 17 FCC Rcd 16825, 16826 (Sept. 12, 2002) (listing the "date of action" authorizing China Netcom's application as September 11, 2002—14 days after acceptance of filing). As part of a government-organized restructuring, effective January 1, 2009, China Netcom, China Netcom USA's parent company, was merged with and into China Unicom. As part of the merger, China Netcom USA was merged into CUA, effective August 31, 2009, and China Netcom USA's Section 214 authorization was assigned to CUA. *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01391, DA 09-2218, 24 FCC Rcd 12611, 12613 (Oct. 15, 2009) ("Notification filed September 30, 2009 of the pro forma assignment of international section 214 authorization, ITC-214-20020728-00361, held by China Netcom (USA) Operations Limited ('China Netcom USA') to China Unicom (Americas) Operations Limited, effective August 31, 2009."). As a result, CUA currently holds two international Section 214 authorizations.
[448] *See, e.g.,* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01331, DA 08-2650, 23 FCC Rcd 17386, 17387 (Dec. 4, 2008) (File No. ITC-T/C-20081114-00499 & ITC-T/C-20081114-00500 referencing a restructuring of ownership interests as a result of China

2017, CUA filed a pro forma notice of transfer of control, when China Unicom Global Limited became the direct owner of CUA following a restructuring of the parent companies.[449] When questioned by Subcommittee staff, Team Telecom officials stated they were not aware of the 2017 filing and could not explain why it did not prompt a security review by Team Telecom.[450] One Team Telecom official noted that the U.S. government's understanding of the risks posed by Chinese state-owned entities evolved over time and that Team Telecom believed the appropriate sequencing was to complete review of China Mobile USA's application before assessing Chinese state-owned carriers with existing authorizations.[451]

Because no security agreement exists between Team Telecom and CUA, Team Telecom is not "directly in privity"[452] with the company and has no insight into its operations.[453] CUA representatives confirmed that it has not engaged with Team Telecom in the nearly 20 years since obtaining Section 214 authorization.[454] Team Telecom officials acknowledged that, without a security agreement, they have no ability to engage CUA.[455] One official suggested that Team Telecom could

---

Unicom's merger with China Netcom); Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01351, DA 09-677, 24 FCC Rcd 3644, 3647 (Mar. 26, 2009) (File No. ITC-T/C-20090204-00082 & ITC-T/C-20090204-00083 referencing restructuring involving China Netcom's merger with China Unicom); Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01391, DA 09-2218, 24 FCC Rcd 12611, 12613 (Oct. 15, 2009) (File No. ITC-ASG-20090930-00433 referencing assignment of China Netcom USA's authorization to CUA); Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Report No. TEL-01396, DA 09-2406, 24 FCC Rcd 13706, 13708 (Nov. 12, 2009) (File No. ITC-214-20020724-00427 referencing that "[b]y letter filed September 30, 2009, Applicant notified the Commission that it changed its name from China Unicom USA Corporation to China Unicom (Americas) Operations Limited (China Unicom Americas), effective August 31, 2009"). Typically, the FCC does not request that Team Telecom review these pro forma notices. FCC PROPOSED EXECUTIVE BRANCH REVIEW REFORM, *supra* note 154, at ¶ 47.

[449] *See* China Unicom (Americas) Operations Limited, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20170301-00025, Attach. 1 (filed Mar. 1, 2017), https://fcc.report/IBFS/ITC-T-C-20170301-00025 (unofficial website); Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01840, DA 17-297, 32 FCC Rcd 2087, 2094 (Mar. 30, 2017). The restructuring "did not change the ultimate ownership or control of [China Unicom Americas] as the [Chinese] government continues to maintain ownership and control over [China Unicom Americas] and will continue to do so." *See* China Unicom (Americas) Operations Limited, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20170301-00025, Attach. 1 (filed Mar. 1, 2017), https://fcc.report/IBFS/ITC-T-C-20170301-00025 (unofficial website).

[450] Briefing with the Dep't of Justice (Apr. 3, 2020); Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020). Officials noted that the FCC does not refer pro forma notices to Team Telecom, *see* Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee); yet, it was a similar notice from CTA that led to its 2007 security agreement.

[451] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020); Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).

[452] Briefing with the Dep't of Justice (Aug. 1, 2019).

[453] *Id.;* Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

[454] Briefing with China Unicom Americas (Apr. 16, 2020).

[455] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).

proactively reach out to CUA and ask questions, but CUA might be unwilling to comply.[456] CUA representatives informed the Subcommittee that the company would engage in discussions with Team Telecom if approached.[457] It has also recently publicly expressed that it "would be willing to engage in discussions with the [FCC] and the other relevant U.S. government agencies regarding . . . an agreement that would be acceptable to resolve any national security concerns."[458]

3. CUA Shares Characteristics Highlighted by Team Telecom about China Mobile USA and CTA

CUA has been providing international telecommunications services pursuant to Section 214 authorizations granted nearly 20 years ago with no oversight by Team Telecom.[459] Nevertheless, CUA and its operations share some similar characteristics with China Mobile USA and CTA.[460] CUA is ultimately majority-owned by the Chinese government, it provides a range of telecommunications services in the United States and can expand those services without further FCC approval, and it has established relationships with major U.S. carriers.

CUA is ultimately majority owned by the Chinese government. China Unicom is a state-owned entity that is ultimately owned by SASAC.[461] SASAC currently owns approximately 98 percent of China Unicom.[462] Over time, China Unicom has added additional ownership layers, including holding companies jointly owned by

---

[456] *Id.*

[457] *See* Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).

[458] *In the Matter of China Unicom (Americas) Operations Limited*, Response to Order to Show Cause, GN Docket No. 20-110, at 15 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-32708&f_number=ITC2142002072800361.

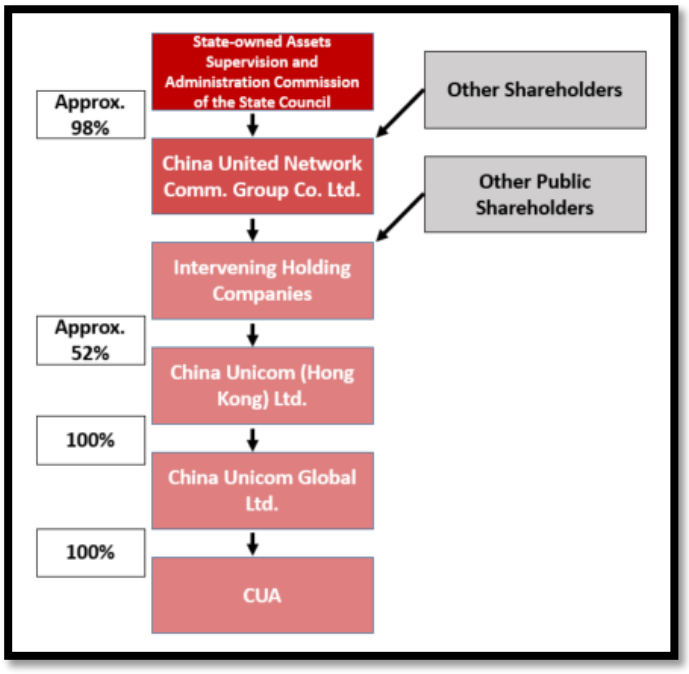
[459] CUA stressed to the Subcommittee that, as a U.S. company, it is subject to U.S. corporate laws, has a good record of compliance with its FCC regulatory obligations, and is willing to cooperate with U.S. law enforcement agencies when asked. *See* Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).

[460] As noted above, CUA explained to the Subcommittee that it also differs significantly from China Mobile USA and CTA with respect to shareholding structure, corporate governance, and history of compliance with the U.S. government. It further noted that there are many government-owned telecommunications carriers operating in the United States with operations and infrastructure similar to CUA. *See* Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).

[461] *See* CHINA UNICOM FY2019 FORM 20-F, *supra* note 434, at 72 (indicating that the ultimate controlling shareholder is Unicom Group, which is controlled by SASAC); *Company Profile*, CHINA UNICOM, https://www.chinaunicom.com.hk/en/about/profile.php; Briefing with China Unicom Americas (Apr. 16, 2020); China Unicom (Americas) Operations Limited, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20170301-00025, Attach. 1 (filed Mar. 1, 2017), https://fcc.report/IBFS/ITC-T-C-20170301-00025 (unofficial website).

[462] *In the Matter of China Unicom (Americas) Operations Limited*, Response to Order to Show Cause, GN Docket No. 20-110, at 18 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-32708&f_number=ITC2142002072800361.

public shareholders.[463] CUA is a wholly-owned subsidiary of China Unicom Global Limited, which is wholly-owned by China Unicom (Hong Kong) Limited.[464] Through multiple intervening holding companies, China Unicom owns approximately 52.1 percent of China Unicom Hong Kong.[465] Thus, China Unicom and the Chinese government—through intermediary companies—own CUA. The diagram below depicts the relevant ownership structure:



[466]

CUA's parent company influences CUA's operations and has access to U.S. customer records. China Unicom Global ("CUG"), which is based in Hong Kong, plays an important role in CUA's operations. It appoints CUA's management team, sets CUA's budget, and provides support for technical solutions, among other

[463] *Id.* at 32. *See also* Briefing with China Unicom Americas (Apr. 16, 2020).
[464] *See generally* China Unicom (Americas) Operations Limited, Notification of Pro Forma Transfer of Control of Section 214 Authority, File No. ITC-T/C-20170301-00025, Attach. 1 (filed Mar. 1, 2017), https://fcc.report/IBFS/ITC-T-C-20170301-00025 (unofficial website).
[465] *In the Matter of China Unicom (Americas) Operations Limited*, Response to Order to Show Cause, GN Docket No. 20-110, at 18 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-32708&f_number=ITC2142002072800361.
[466] The diagram is based on information from the following: CHINA UNICOM FY2019 FORM 20-F, *supra* note 434; *Company Profile*, CHINA UNICOM, https://www.chinaunicom.com.hk/en/about/profile.php; Briefing with China Unicom Americas (Apr. 16, 2020); *In the Matter of China Unicom (Americas) Operations Limited*, Response to Order to Show Cause, GN Docket No. 20-110, at Exhibit 2 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-32708&f_number=ITC2142002072800361.

items.[467] CUA also consults with its parent company before establishing any point of presence in the United States.[468]

CUG also manages CUA's U.S. customer records. According to a CUA representative, customer records are stored on servers in Hong Kong and maintained by CUG.[469] CUA and CUG have signed a confidentiality agreement that governs access to the records and also establishes procedures to protect customer proprietary network information.[470] Access to U.S. records is governed by this agreement, which includes requiring those seeking access to have a business justification; however, CUA representatives suggested that CUG decides what constitutes a sufficient justification.[471] When questioned about this arrangement, CUA representatives explained that it is necessary for CUG to have access to all customer records given the nature of the international services provided by CUG's subsidiaries.[472] The representatives described this treatment as "common among international carriers."[473] They also indicated that, for enterprise customers, the information shared between affiliates is that which is necessary for provisioning and customer service.[474] For mobile virtual network operator ("MVNO") services, CUA chooses to use a service platform in Hong Kong because "the subscriber base does not warrant a standalone U.S. platform."[475]

CUA also informed the Subcommittee that its parent company monitors CUA's network operations to ensure that the global network is performing consistently.[476] CUA also leverages CUG's network operations center, located in Hong Kong, for technical support.[477] CUA engineers manage CUA's U.S.-based network equipment; however, representatives confirmed that CUG can remotely configure CUA's network equipment.[478]

---

[467] Briefing with China Unicom Americas (Apr. 16, 2020). *See also In the Matter of China Unicom (Americas) Operations Limited*, Response to Order to Show Cause, GN Docket No. 20-110, at 20 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-32708&f_number=ITC2142002072800361.
[468] Briefing with China Unicom Americas (Apr. 16, 2020).
[469] *Id.*
[470] *Id. See also* Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[471] Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee); Briefing with China Unicom Americas (Apr. 16, 2020).
[472] Briefing with China Unicom Americas (Apr. 16, 2020).
[473] *Id.*
[474] Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[475] *Id.*
[476] Briefing with China Unicom Americas (Apr. 16, 2020).
[477] *Id.*
[478] Letter from Squire Patton Boggs, counsel to CUA, to the Subcommittee (Apr. 29, 2020) (on file with the Subcommittee).

CUA provides a range of communications services in the United States with its Section 214 authorizations. Like CTA, CUA is an international common carrier authorized to provide facilities-based and resale-based services.[479] Under its Section 214 authorizations, CUA may provide "international basic switched, private line, data, television and business services" directly through its own facilities or by reselling the services of any other authorized common carrier.[480] CUA informed the Subcommittee that it primarily resells the services of U.S. carriers, given that it does not own transmission infrastructure within the United States.[481]

CUA offers "reliable end-to-end global integrated telecommunication services and solutions" and "provides personal customers with premium voice and mobility services."[482] CUA advertises that it provides a range of services, including global connectivity services, global internet access, cloud, video conferencing, and content and security services.[483] As highlighted by Team Telecom in connection with CTA, some of these services are regulated by Section 214 and others are not.[484] For example, CUA operates as a MVNO, reselling mobile services of major U.S. providers to retail customers.[485] CUA's retail customers are primarily Chinese speaking individuals visiting or living in the United States.[486] CUA offers a "one-card-multiple-number" service that provides customers in the United States with a Chinese telephone number so that individuals in China can call the Chinese number to reach the U.S. customer without paying international toll charges.[487] U.S. customers in the United States can also use the service to call China using a local number.[488]

---

[479] *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00581, DA 02-2500, 17 FCC Rcd 19181, 19182 (Oct. 3, 2002). *See also* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00576, DA 02-2234, 17 FCC Rcd 16825, 16826 (Sept. 12, 2002) (China Netcom USA's 2002 authorization). China Netcom USA's authorization was subsequently assigned to CUA. *See* Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01391, DA 09-2218, 24 FCC Rcd 12611, 12613 (Oct. 15, 2009).

[480] 47 C.F.R. § 63.22(d) (facilities-based international common carrier); 47 C.F.R. § 63.23(c) (resale-based international common carrier).

[481] Briefing with China Unicom Americas (Apr. 16, 2020).

[482] *About—China Unicom Americas*, LINKEDIN, https://www.linkedin.com/company/china-unicom-americas.

[483] *Id.*

[484] Briefing with China Unicom Americas (Apr. 16, 2020); *Executive Branch Recommendation re CTA*, *supra* note 56, at 7–9 (Apr. 9, 2020).

[485] Briefing with China Unicom Americas (Apr. 16, 2020).

[486] *Id.*

[487] *Id.*; Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).

[488] Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).

CUA also provides a range of business data services, including international private lines and lease circuits.[489] According to CUG's website, private lines provide customers "end to end dedicated and permanent digital point to point connectivity between two regions."[490] CUA also provides end-to-end connectivity through international Ethernet connections and multi-protocol label switching ("MPLS") VPN.[491] MPLS VPN is either "built on the IP carrier network" or uses a "series of virtual switches leased to" customers to allow them to securely transmit data, such as internal data, voices, images and videos, between different locations.[492]

CUA's primary business line is broadband internet services for customers in both the United States and China.[493] CUG "ha[s] direct connection[s] to major [internet service providers] in many countries makes [*sic*] Internet access faster and minimizes distance delays."[494] CUA informed the Subcommittee that it peers with 26 IP partners for the exchange of internet traffic.[495] CUA also provides data center, and cloud computing services,[496] for which Section 214 authorization is not needed.[497]

To provide these services, CUA has established 11 points of presence—five on the East coast, five on the West coast, and one in the Midwest.[498] The points of presence consist of CUA-owned routers installed in colocation facilities leased from third-parties.[499] China Unicom also advertises that it operates points of presence across the world, specifically mentioning the locations in Los Angeles, New York, and San Jose, which "provide . . . for customer and partner network interconnections."[500] In fact, China Unicom promotes its international MPLS VPN

---

[489] Briefing with China Unicom Americas (Apr. 16, 2020). *See also Customer Solutions*, CHINA UNICOM GLOBAL, at 15, https://www.chinaunicomglobal.com/group1/M00/00/08/CngaWFo0fQOAfarRAPYieoOnUf8345.pdf.
[490] *See Customer Solutions*, CHINA UNICOM GLOBAL, at 15, https://www.chinaunicomglobal.com/group1/M00/00/08/CngaWFo0fQOAfarRAPYieoOnUf8345.pdf.
[491] Briefing with China Unicom Americas (Apr. 16, 2020). In its recommendation to revoke CTA's authorizations, Team Telecom described MPLS VPN services as falling into a "regulatory gray area." *Executive Branch Recommendation re CTA*, *supra* note 56, at 7–9 (Apr. 9, 2020).
[492] *See MPLS VPN*, CHINA UNICOM GLOBAL, https://www.chinaunicomglobal.com/hk/mplsvpn.
[493] Briefing with China Unicom Americas (Apr. 16, 2020).
[494] *See Customer Solutions*, CHINA UNICOM GLOBAL, at 25, https://www.chinaunicomglobal.com/group1/M00/00/08/CngaWFo0fQOAfarRAPYieoOnUf8345.pdf.
[495] Briefing with China Unicom Americas (Apr. 16, 2020); Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[496] Briefing with China Unicom Americas (Apr. 16, 2020). CUA resells the services of a data center provider. It does not own, control, or manage the data center itself. *Id.*
[497] *Executive Branch Recommendation re CTA*, *supra* note 56, at 10.
[498] Briefing with China Unicom Americas (Apr. 16, 2020). The points of presence are located in (1) Seattle, WA; (2) Hillsboro, OR; (3) Palo Alto, CA; (4) San Jose, CA; (5) Los Angeles, CA; (6) Dallas, TX; (7) Reston, VA; (8) Ashburn, VA; (9) Chicago, IL; (10) New York, NY; and (11) Miami, FL.
[499] *Id.* The routers are used for CUA's 3 IP data networks. *Id.*
[500] *See Customer Solutions*, CHINA UNICOM GLOBAL, at 17, https://www.chinaunicomglobal.com/group1/M00/00/08/CngaWFo0fQOAfarRAPYieoOnUf8345.pdf.

service, noting that through its "international network and comprehensive worldwide partnerships, [its] global MPLS VPN service allows customers to gain access to extensive international network infrastructure, in-country facilities and committed services[,] and support resources."[501]

CUA has built relationships with major U.S. carriers. CUA does not own transmission networks in the United States.[502] It leases transmission circuits from major U.S. carriers for data capacity between CUA's points of presence, as well as between those points of presence and CUA's end customers.[503] Through these connections, CUA ensures that its U.S.-based customers can connect between the United States and China, or other international points.[504] CUA informed the Subcommittee that its U.S. carrier partners operate the same way to reach U.S. customers in China. For example, a U.S. carrier with customers in mainland China would lease network capacity in China from China Unicom to connect to the U.S. carrier's end-customer.[505]

CUA has established relationships with AT&T, Verizon, and CenturyLink, among other U.S. carriers.[506] These relationships include the provision of network or other retail services.[507] Verizon maintains an interconnection agreement and peering arrangement with CUA, as well as separate agreements with its Chinese parent companies.[508] AT&T sells voice and data transport services, which CUA uses to provide services to its customers in the United States.[509] Although it did not specify the particular services sold to CUA, CenturyLink informed the Subcommittee that it has limited commercial relationships with all of the Chinese carriers, which include selling network services, circuits, or collocation services.[510]

---

[501] *See id.* at 19.
[502] Briefing with China Unicom Americas (Apr. 16, 2020).
[503] *Id.*; Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[504] Briefing with Verizon (Sept. 4, 2019); Briefing with AT&T (Sept. 17, 2019); Briefing with CenturyLink (Sept. 10, 2019).
[505] Briefing with China Unicom Americas (Apr. 16, 2020); Email from Squire Patton Boggs, counsel to CUA, to the Subcommittee (June 3, 2020) (on file with the Subcommittee).
[506] Briefing with Verizon (Sept. 4, 2019); Briefing with AT&T (Sept. 17, 2019); Briefing with CenturyLink (Sept. 10, 2019).
[507] Briefing with Verizon (Sept. 4, 2019); Briefing with AT&T (Sept. 17, 2019); Briefing with CenturyLink (Sept. 10, 2019).
[508] Briefing with Verizon (Sept. 4, 2019).
[509] Briefing with AT&T (Sept. 17, 2019). As with CTA, AT&T representatives told the Subcommittee that the revenue generated by its agreements with CUA is relatively small, particularly when compared to similar agreements with other large international carriers. For example, similar arrangements with other large international carriers generate up to 36 to 62 times as much revenue as arrangements with the Chinese state-owned carriers discussed in this report. *Id.*; Email from Gibson, Dunn & Crutcher LLP, counsel to AT&T, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[510] Briefing with CenturyLink (Sept. 10, 2019).

These services allow CUA to deliver traffic from a CUA point of presence through CenturyLink's network to a CUA customer located in the United States.[511]

Neither Verizon, AT&T, nor CenturyLink maintains any mitigation or other agreement focused on network security with CUA.[512] As noted above, however, the U.S. carriers employ security measures that apply regardless of whether an interconnection agreement exists.[513]

* * * * *

On April 24, 2020, the FCC issued an order requiring CUA to demonstrate why its Section 214 authorizations should not be revoked.[514] CUA responded to the order on June 1, 2020.[515] CUA argued that it has complied with FCC regulations and provided quality services to its customers for over two decades.[516] Further, CUA stressed that it is subject to U.S. corporate laws and has "demonstrated willingness to cooperate with U.S. law enforcement agencies when asked."[517] CUA also argued that the federal government has not highlighted any CUA activity that might endanger national security, aside from partial and indirect ownership by the Chinese government.[518] The latter, according to CUA, is not a sufficient basis for revocation.[519] Finally, CUA detailed why it is not subject to exploitation, influence, or control by the Chinese government.[520] The FCC is evaluating the information CUA submitted and considering whether to revoke its authorizations.

Similarly, in anticipation of this report being released, CUA submitted a letter to the Subcommittee seeking to distinguish CUA from "other, similar companies in the market in terms of shareholding structure, corporate governance,

---

[511] *Id.* CenturyLink purchases the same network services from the Chinese carriers in China, to allow CenturyLink to deliver traffic to a CenturyLink customer based in China. *Id.*
[512] *See* Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019). Verizon representatives indicated that the company's contractual agreements with CUA are substantially identical to those it maintains with other carriers. Teleconference with Verizon (June 2, 2020).
[513] Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Briefing with AT&T (Sept. 17, 2019); Teleconference with Verizon (June 2, 2020); Email from CenturyLink to the Subcommittee (June 2, 2020) (on file with the Subcommittee); Email from Gibson, Dunn & Crutcher LLP, counsel to AT&T, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[514] *See In the Matter of China Unicom (Americas) Operations Limited*, Order to Show Cause, DA 20-449 (Apr. 24, 2020), https://docs.fcc.gov/public/attachments/DA-20-449A1.pdf.
[515] *See In the Matter of China Unicom (Americas) Operations Limited*, Response to Order to Show Cause, GN Docket No. 20-110 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=-32708&f_number=ITC2142002072800361.
[516] *Id.* at i.
[517] *Id.* at ii.
[518] *Id.* at ii, 2.
[519] *Id.* at 9–10.
[520] *Id.* at 30–32.

and other areas."[521] In the letter, CUA reiterated many of the points made in its response to the FCC's show cause order. This includes that CUA has complied with U.S. laws, has never been accused of criminal conduct or violation of FCC regulations, and is not subject to the exploitation, influence, or control of the Chinese government.[522] The letter also details CUG's and China Unicom Hong Kong's independence and describes recent actions taken by CUA to strengthen its corporate governance and compliance program.[523]

D. ComNet (USA) LLC and Pacific Networks Corp.

ComNet (USA) LLC ("ComNet") (formerly known as CM Tel (USA) LLC[524]) is a telecommunications service provider that "offer[s] telecom partners and operators international termination services, calling card[s] and global SIM card[s]."[525] Its website also states that it provides "enterprise business phones system, [messaging], managed network and IT service, website and WeChat related development, etc."[526] ComNet (then CM Tel (USA) LLC) was incorporated in Delaware in July 1999.[527] At that time, the company was a subsidiary of CM Telecom International Limited, a Hong Kong based company.[528] In 2009, ComNet was acquired by CITIC Telecom International Holdings Limited ("CITIC"),[529] which describes itself as one of Asia Pacific's leading telecommunications service providers of "mobile international roaming, international voice, international SMS, international data and international value-added telecommunications services, etc.

---

[521] Letter from Squire Patton Boggs to Rob Portman, Chairman, Permanent Subcomm. on Investigations, and Tom Carper, Ranking Member, Permanent Subcomm. on Investigations (June 3, 2020).
[522] *Id.*
[523] *Id.*
[524] CM Tel (USA) LLC changed its name to ComNet in 2009. *See* ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee).
[525] *About Us*, COMNET (USA) LLC, https://www.comnet-telecom.us/about-us. ComNet resells SIM cards of mobile wireless companies; it does not provide wireless service over its network. Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[526] *See ComNet (USA) LLC*, LINKEDIN, https://www.linkedin.com/company/comnet-telecom.
[527] COMNET (USA) LLC, STATEMENT OF INFORMATION FOR THE FISCAL YEAR ENDED DEC. 31, 2018 (LLC-12) FILED WITH THE SEC'Y OF STATE OF THE STATE OF CALIFORNIA, FILE NO. 19-C86032 (July 29, 2019), https://businesssearch.sos.ca.gov/Document/RetrievePDF?Id=199920510003-26628618; ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee).
[528] *See* In the Matter of CM Tel (USA) LLC Application for Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, for Global Authority to Operate as an International Facilities-Based and Resale Carrier (Sept. 27, 1999), https://fcc.report/IBFS/ITC-214-19990927-00607 (unofficial website).
[529] *See* CITIC PACIFIC, ANNUAL REPORT 183 (2010), https://www.citic.com/uploadfile/2017/0525/20170525102539646.pdf ("In 2009 a listed subsidiary group of the Company CITIC Telecom acquired the remaining 51% equity interest in CM Tel (USA) LLC (renamed as ComNet (USA) LLC in July 2009 . . . ."). At this time, CM Tel (USA) LLC formally changed its name to ComNet (USA) LLC. ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee).

to global carriers."[530] At the time CITIC acquired ComNet, it also owned Pacific Networks Corp. ("Pacific Networks"), another U.S. company.[531] In integrating ComNet into its corporate organization, CITIC made ComNet a wholly-owned subsidiary of Pacific Networks.[532]

The integration of the companies prompted Team Telecom to enter into a security agreement with the companies in March 2009. Yet, like CTA, Team Telecom has exercised minimal oversight of the companies and their operations in the United States—relying on intermittent email communication and completing only two site visits in more than ten years.

1. ComNet's Initial Section 214 Authorization Did Not Require Team Telecom's Review

ComNet (then CM Tel (USA) LLC) applied for international Section 214 authorization in 1999 to provide global international facilities-based and resale services between the United States and all international points.[533] ComNet certified that it had no affiliation with any foreign or U.S. facilities-based carrier.[534] The FCC did not refer the application to Team Telecom. The application was accepted for filing on October 13, 1999[535] and granted on October 27, 1999.[536]

---

[530] *Corporate Profile*, CITIC TELECOM INTERNATIONAL, https://www.citictel.com/about-us/corporate-profile/.
[531] *See* CM Tel (USA) LLC, Application for Transfer of Control of International Section 214 Authority, File No. ITC-T/C-20080913-00428, Attach. 1 (filed Sept. 13, 2008), https://fcc.report/IBFS/ITC-T-C-20080913-00428 (unofficial website); CM Tel (USA) LLC, Application for Transfer of Control of International Section 214 Authority, File No. ITC-T/C-20080913-00428, Supplement (filed Sept. 25, 2008), https://fcc.report/IBFS/ITC-T-C-20080913-00428 (unofficial website) (stating "CITIC 1616 [Holdings Limited] will acquire CM Tel (USA) LLC through CITIC 1616's indirectly wholly owned subsidiary, Pacific Networks Corp.").
[532] *See* CM Tel (USA) LLC, Application for Transfer of Control of International Section 214 Authority, File No. ITC-T/C-20080913-00428, Attach. 1 (filed Sept. 13, 2008), https://fcc.report/IBFS/ITC-T-C-20080913-00428 (unofficial website).
[533] *See* In the Matter of CM Tel (USA) LLC Application for Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended, for Global Authority to Operate as an International Facilities-Based and Resale Carrier (Sept. 27, 1999), https://fcc.report/IBFS/ITC-214-19990927-00607 (unofficial website).
[534] *See id.* at 5.
[535] Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-00144S, at 2 (Oct. 13, 1999).
[536] Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-00151, DA No. 99-2328, 14 FCC Rcd 17862, 17864 (Oct. 28, 1999) (listing the "date of action" authorizing the application as October 27, 1999).

2. Pacific Networks' Initial Section 214 Authorization Prompted Team Telecom Review and Resulted in a Security Agreement

Pacific Networks applied for international Section 214 authorization in 2007 to provide international resale services between the United States and permissible international points, including China, solely by reselling unaffiliated U.S. facilities-based carriers' international switched services.[537] Although not majority owned, Pacific Networks disclosed that it was affiliated with the Chinese government, which held a 14 percent indirect ownership (29 percent attributable interest) in Pacific Networks through numerous intervening foreign organized holding companies.[538] The FCC referred the application to Team Telecom on September 14, 2007.[539]

Unlike the initial CTA and CUA applications, Team Telecom requested that Pacific Networks' application be removed from streamlining.[540] It engaged Pacific Networks to better understand the company's existing and anticipated activities, employees, and infrastructure.[541] Pacific Networks informed Team Telecom that it was not providing services to customers within the United States at the time it applied for Section 214 authorization.[542] However, Pacific Networks anticipated providing "international resold voice and data service for U.S. customers," including voice and SMS services, resale of leased circuit services, and internet exchange services.[543] Pacific Networks further explained that it planned to establish three points of presence within the United States—two in California and one in New York—and to interconnect with Qwest to relay calls to other carriers.[544] Pacific Networks indicated that it would not directly provide access to the public switched telephone network, but rather make such connections available through other local carriers, including AT&T and Qwest.[545] In addition to its written responses, Pacific Networks provided copies of its standing operating procedures for its network operations center, interface control documents, SMS service description, list of equipment, and point of presence configurations.[546]

Nearly a year after the FCC referred the application, in September 2008, Team Telecom alerted the FCC that it had completed its review and had no

---

[537] *See* Pacific Networks Corp., International Section 214 Application File No. ITC-214-20070907-00368, https://fcc.report/IBFS/ITC-214-20070907-00368/590946 (unofficial website). *See also* DHS00460PSI.
[538] Pacific Networks Corp., International Section 214 Application File No. ITC-214-20070907-00368, at Attach. 1, https://fcc.report/IBFS/ITC-214-20070907-00368/590946 (unofficial website).
[539] FCC-PSI-000412–13.
[540] FCC-PSI-000415.
[541] *Cf.* TT-DOJ-045–60.
[542] *See id.* at TT-DOJ-045.
[543] *See id.*
[544] *Id.* at TT-DOJ-056.
[545] *Id.* at TT-DOJ-056–57.
[546] *See generally* TT-DOJ-061–101.

objection to the FCC approving the application, provided that the FCC condition its approval on Pacific Networks' agreement to abide by the commitments and undertakings it made to DOJ, and DHS.[547] Those commitments and undertakings were outlined in a September 2, 2008 letter from Pacific Networks to Team Telecom, which included some of the same commitments contained in CTA's 2007 security agreement.[548] For example, among other items, Pacific Networks committed to (1) ensuring that U.S. records were made available in response to lawful U.S. process; (2) ensuring that U.S. records were not "made subject to mandatory destruction" under foreign laws; (3) take all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. records; (4) maintain a point of contact within the United States with the authority and responsibility for accepting and overseeing compliance with a lawful demand by U.S. law enforcement authorities; and (5) notify DOJ and DHS of any material changes in any of the facts in the security agreement, including any increase or decrease in foreign government control.[549] The FCC granted Pacific Networks' application effective September 3, 2008, conditioned on Pacific Networks abiding by its commitments to Team Telecom.[550]

3. ComNet's Integration with Pacific Networks Prompted Further Team Telecom Scrutiny and Resulted in a Security Agreement

As noted above, CITIC acquired ComNet and made ComNet a wholly-owned subsidiary of Pacific Networks.[551] In connection with this organizational change, ComNet sought FCC approval to transfer control of a portion of its 1999 Section 214 authorization to Pacific Networks—specifically, with respect to the U.S.-China and U.S.-Hong Kong routes, the authority to provide switched services through the resale of unaffiliated U.S. facilities-based carriers' international switched

---

[547] In the Matter of Pacific Networks Corp. Application for Authority to Provide Switched Resale Service Between the United States and Permissible Int'l Points (File No. ITC-214-20070907-00368) – Petition to Adopt Conditions to Authorizations and Licenses (filed Sept. 3, 2008), https://fcc.report/IBFS/ITC-214-20070907-00368/661672 (unofficial website).

[548] Letter from Yuen Kee Tong, Chairman, Pacific Networks Corp., to Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec., & Patrick Rowan, Acting Assistant Att'y Gen. for Nat'l Sec., Dep't of Justice (Sept. 2, 2008).

[549] *Id.*

[550] Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01304, DA No. 08-2037, 23 FCC Rcd 13265, 13266 (Sept. 4, 2008) (listing the "date of action" authorizing the application as September 3, 2008).

[551] CM Tel (USA) LLC, Application for Transfer of Control of International Section 214 Authority, File No. ITC-T/C-20080913-00428, Attach. 1 (filed Sept. 13, 2008), https://fcc.report/IBFS/ITC-T-C-20080913-00428 (unofficial website).

services.[552] The FCC referred ComNet's transfer of control application to Team Telecom for review.[553]

In December 2008, Pacific Networks filed a notice of surrender of its September 2008 Section 214 authorization with the FCC.[554] Pacific Networks claimed the surrender was the result of "necessary financial circumstances" leading Pacific Networks' indirect parent company to undergo "a transfer of control that cannot be delayed pending Commission approval."[555] The relevant transfer of control involved a consolidation of some CITIC holding companies, resulting in the Chinese government acquiring a greater interest in CITIC, and by extension Pacific Networks and ComNet.[556]

In January 2009, Pacific Networks applied for a new international Section 214 authorization.[557] This time, Pacific Networks sought authority to provide resale services to all international routes.[558] It subsequently clarified with the FCC that it sought authority to provide resale service on all U.S. routes except to China and Hong Kong; with respect to those two locations, the company would be authorized to

---

[552] *Id.*; Letter from Joshua T. Guyan to Fed. Commc'ns Comm'n Int'l Bureau (Apr. 22, 2009). Resale could be done directly or indirectly through the resale of another U.S. resale carrier's international switched services.

[553] FCC-PSI-000154–55. At the time the transfer request was sent to Team Telecom, the Chinese Government held a 14 percent indirect ownership (29 percent attributable interest) in ComNet through various intervening companies, and therefore, ComNet was considered "affiliated with Chinese carriers owned or controlled by the Chinese Government." *See id.* The Chinese government increased its indirect holdings in CITIC in January 2009, as described more below.

[554] *See* Letter from Joshua T. Guyan to Fed. Commc'ns Comm'n Int'l Bureau (Dec. 23, 2008).

[555] *See id.* Prior to surrendering the authorization, Pacific Networks filed for special temporary authority to "transfer control of Pacific Networks Corporation from CITIC Pacific Limited to CITIC Group pending Commission action on an underling transfer of control application." *See* FCC-PSI-000510–26. Pacific Networks indicated that the transfer of control was necessary to strengthen its liquidity due to certain realized losses and was unrelated to telecommunications services. *See* FCC-PSI-000510–26. It appears that the FCC did not rule on the special temporary authority request prior to Pacific Networks surrendering its authorization. The FCC issued a public notice of the surrender on January 2, 2009. Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01335, DA 09-2, 24 FCC Rcd 16, 19–20 (Jan. 2, 2009) (listing the effective date of the surrender as Dec. 23, 2008).

[556] *Compare* Pacific Networks Corp., International Section 214 Application File No. ITC-214-20070907-00368, Attach. 1, https://fcc.report/IBFS/ITC-214-20070907-00368 (unofficial website) (referencing the Chinese Government's 14 percent indirect ownership (29 percent attributable interest)) *with* Pacific Networks Corp., International Section 214 Application File No. ITC-214-20090105-00006, Attach. 1, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=76226&acct=575631&id_form_num=2&filing_key=-158718 (referencing the Chinese government's 57.6 percent attributable interest).

[557] *See* Pacific Networks Corp., International Section 214 Application File No. ITC-214-20090105-00006, https://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/attachment_menu.hts?id_app_num=76226&acct=575631&id_form_num=2&filing_key=-158718; Fed. Commc'ns Comm'n, *Public Notice – International Applications Accepted for Filing*, Rep. No. TEL-01338S, at 2 (Jan. 16, 2009).

[558] *Id.*

provide switched services, either directly or indirectly through the resale of another U.S. resale carrier's international switched services.[559] The FCC referred Pacific Networks' application to Team Telecom for review.[560]

Team Telecom engaged both ComNet and Pacific Networks on perceived national security risks associated with their applications.[561] Team Telecom's questions focused on the companies' integration, as well as their creation of operating and security procedures to protect against unauthorized access to, or disclosure of, U.S. records.[562] Team Telecom also sought to ensure the companies had identified a law enforcement point of contact.[563]

Ultimately, Team Telecom determined that the risks it identified could be mitigated through a security agreement, signed jointly by ComNet and Pacific Networks.[564] The companies, along with DHS and DOJ, executed the agreement on March 3, 2009.[565] The agreement included many of the same general provisions as other security agreements, as well as certain new requirements. This included, among others (1) making U.S. records available within the United States in response to lawful U.S process; (2) providing DHS and DOJ with descriptions of the companies' physical and logical technical security architecture, security policies and standards, and information technology governance controls; (3) ensuring that U.S. records are not made subject to mandatory destruction under any foreign laws; (4) taking all practicable measures to prevent unauthorized access to, or disclosure of the content of, communications or U.S. records; (5) maintaining at least one point of contact within the United States to oversee compliance with law enforcement requests; (6) notifying DOJ and DHS of changes to services, ownership, or operations; (7) notifying DOJ and DHS of any malicious cybersecurity attacks detected on systems used to provide services within the U.S. domestic

---

[559] *See* Letter from Joshua T. Guyan to Fed. Commc'ns Comm'n Int'l Bureau (Apr. 22, 2009).
[560] FCC-PSI-000478–79.
[561] *Cf.* DHS00460PSI (noting that the security agreement signed with ComNet in 2009 took into account (1) ComNet's transfer of control application and (2) Pacific Networks' new Section 214 application).
[562] *See* TT-DOJ-120–22.
[563] *See id.*
[564] In the Matter of CM Tel (USA) (File No. ITC-T/C-20080913-00428), In the Matter of Pacific Networks Corp. (File No. ITC-214-20090105-00006) – Petition to Adopt Conditions to Authorizations and Licenses (Mar. 30, 2009), https://fcc.report/IBFS/ITC-T-C-20080913-00428/704912 (unofficial website); Letter from Norman Yuen, Chairman, Pacific Networks Corp., & Fan Wei, Dir., CM Tel (USA) LLC to Stephen Heifetz, Deputy Assistant Sec'y for Policy Dev., Dep't of Homeland Sec. & Matthew Olsen, Acting Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Justice (Mar. 3, 2009).
[565] Letter from Norman Yuen, Chairman, Pacific Networks Corp., & Fan Wei, Dir., CM Tel (USA) LLC to Stephen Heifetz, Deputy Assistant Sec'y for Policy Dev., Dep't of Homeland Sec. & Matthew Olsen, Acting Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Justice (Mar. 3, 2009). *See also* In the Matter of CM Tel (USA) (File No. ITC-T/C-20080913-00428), In the Matter of Pacific Networks Corp. (File No. ITC-214-20090105-00006) – Petition to Adopt Conditions to Authorizations and Licenses (Mar. 30, 2009), https://fcc.report/IBFS/ITC-T-C-20080913-00428/704912 (unofficial website).

communications infrastructure; and (8) agreeing to allow DOJ and DHS to visit any domestic facility within 48 hours' notice.[566]

On March 30, 2009, Team Telecom informed the FCC that it had no objection to the FCC approving the applications, provided that the FCC condition approval on ComNet and Pacific Networks abiding by the commitments and undertakings listed in the March 3, 2009 agreement.[567] The FCC granted the authorizations in April 2009.[568]

4. Despite a Security Agreement, Team Telecom Conducted Limited Post-Authorization Monitoring

Team Telecom's oversight of ComNet in the 11 years since executing the security agreement has been minimal.[569] Neither DOJ nor DHS were able to locate any communications demonstrating Team Telecom's engagement of ComNet prior to 2012. In 2009 and 2010, Team Telecom's monitoring consisted of receiving unprompted written updates from ComNet.[570] For example, in November 2009, ComNet notified Team Telecom about changes in CITIC's board of directors.[571] In 2010, ComNet alerted Team Telecom as to its name change from CM Tel to ComNet and also provided Team Telecom with a new law enforcement point of contact.[572] Neither DOJ nor DHS were able to locate any communications with ComNet in 2011.

---

[566] *See generally* Letter from Norman Yuen, Chairman, Pacific Networks Corp., & Fan Wei, Dir., CM Tel (USA) LLC to Stephen Heifetz, Deputy Assistant Sec'y for Policy Dev., Dep't of Homeland Sec. & Matthew Olsen, Acting Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Justice (Mar. 3, 2009).

[567] In the Matter of CM Tel (USA) (File No. ITC-T/C-20080913-00428), In the Matter of Pacific Networks Corp. (File No. ITC-214-20090105-00006) – Petition to Adopt Conditions to Authorizations and Licenses (Mar. 30, 2009), https://fcc.report/IBFS/ITC-T-C-20080913-00428/704912 (unofficial website).

[568] Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01357, DA 09-1030, 24 FCC Rcd 5376, 5379 (May 7, 2009) (listing the "date of action" authorizing the transfer as April 24, 2009); Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01353, DA 09-799, 24 FCC Rcd 4155, 4156 (Apr. 9, 2009) (listing the "date of action" authorizing the application as April 8, 2009) (corrected Fed. Commc'ns Comm'n, *Public Notice – International Authorizations Granted*, Rep. No. TEL-01355, DA 09-898, 24 FCC Rcd 6379, 6384 (Apr. 23, 2009)).

[569] In discussions with the Subcommittee and its response to the FCC's Show Cause Order, ComNet stressed that it has regularly updated Team Telecom on its operations, provided a substantial amount of information to the agencies, and always responded to promptly to requests for information. *See* Briefing with ComNet (Apr. 13, 2020); Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee); *In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Response to Order to Show Cause, GN Docket No. 20-111, at 7–9, Exhibit K (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=710677&f_number=ITC2142009042400199.

[570] *See, e.g.*, TT-DOJ-309–18; DHS00133PSI–44.

[571] TT-DOJ-309–17.

[572] TT-DOJ-318.

In 2012, Team Telecom proactively engaged ComNet. After ComNet alerted Team Telecom about a corporate restructuring of its parent company,[573] a DHS official sent ComNet written inquiries and deliverable requests.[574] The requests sought information related to ComNet's (1) technical architecture; (2) security policies and standards; (3) governance controls for its U.S. facility; (4) law enforcement point of contact; (5) operational and IT auditing; and (6) other confirmations relating to the requirements outlined in the 2009 security agreement.[575] ComNet provided this information.[576] Officials informed the Subcommittee that Team Telecom determined no further action was required, as nothing ComNet provided suggested non-compliance with the terms of the security agreement.[577] In 2013, Team Telecom again asked for a "brief, up-to-date company overview."[578]

For approximately five years after signing the security agreement with ComNet, Team Telecom relied on these written representations as to ComNet's compliance with the 2009 security agreement. Although one official explained that Team Telecom generally waited to visit the offices of Chinese carriers with existing Section 214 authorizations during consideration of China Mobile USA's application,[579] Team Telecom conducted a site visit to ComNet's offices in February 2014.[580] A memo summarizing the 2014 visit suggests that the meeting may have been prompted by CITIC's application for Section 214 authority.[581] That application was referred to Team Telecom for review, and "in light of the pre-existing agreement with [Pacific Networks] and ComNet, [Team Telecom] determined a visit to . . . ComNet's domestic facility to be in order."[582]

Team Telecom met with representatives from ComNet and CITIC to discuss ComNet's corporate structure, telecommunications infrastructure, security policies and procedures, and law enforcement processes.[583] ComNet generally noted that no

---

[573] DHS00159PSI–60; DHS00176PSI–77.
[574] *Cf.* DHS00178PSI–81 (referencing a July 23, 2012 email from Team Telecom requesting particular deliverables) (attachments omitted).
[575] *Id.*
[576] DHS00178PSI–311.
[577] Email from the Dep't of Homeland Sec. to the Subcommittee (June 4, 2020) (on file with the Subcommittee).
[578] *See In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Response to Order to Show Cause, GN Docket No. 20-111, at Exhibit K (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=710677&f_number=ITC2142009042400199 (Letter from Bruce Olcott, Counsel to ComNet & Pacific Networks, to Hunter Deeley, Foreign Investment Review Staff, Nat'l Sec. Div., Dep't of Justice (Oct. 10, 2013)).
[579] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).
[580] DHS00460PSI–465. Although not a party to the 2009 security agreement, a representative from the Department of Defense's Chief Information Office also attended the site visit. *See id.* at DHS00460PSI.
[581] *Id.* at DHS00461PSI.
[582] *Id.*
[583] *See generally* DHS00460PSI–65.

ownership changes had occurred since it executed the 2009 security agreement.[584] ComNet represented during the meeting that the Chinese government had "passive" involvement in the company's day-to-day operations, providing no input into operational decision-making.[585] In terms of law enforcement processes, ComNet confirmed its ability to implement call monitoring within one hour of a lawful requests.[586] The call monitoring included determining telephone numbers of call parties and monitoring specific calling card accounts.[587]

Ultimately, Team Telecom made no findings or recommendations specific to ComNet. The memo noted that Team Telecom should

> reassess [its] collective strategy in dealing with foreign state-owned companies . . . that provide telecommunications services in the United States. Further recommendations regarding [ComNet's] license are pending the completion of [Team Telecom's] ongoing comprehensive review of foreign state-owned companies holding telecommunications licenses in coordination with the FCC.[588]

According to one official, the recommendation was a reference to Team Telecom's review of China Mobile USA's application and reflected Team Telecom's evolving understanding regarding foreign state-owned companies, particularly Chinese companies.[589]

Between March 2014 and late 2017, Team Telecom officials provided the Subcommittee with one communication with ComNet—a July 2015 letter ComNet submitted in response to a Team Telecom request for an update on any operational changes since the February 2014 site visit.[590] In September 2017, Team Telecom contacted ComNet's external counsel, who confirmed "ComNet and Pacific Networks . . . remain in operation."[591] A month later, Team Telecom requested

---

[584] *Id.* at DHS00460PSI–61.
[585] *Id.* at DHS00462PSI. ComNet informed the Subcommittee that it has "consistently" informed Team Telecom and the FCC that the Chinese government has indirect ownership in the companies, has not been involved in operational decision-making, and has not been involved "passive or otherwise" in ComNet's or Pacific Networks' day-to-day operations. Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[586] DHS00460PSI–465, at DHS00464PSI.
[587] DHS00460PSI–465.
[588] *Id.* at DHS00460PSI.
[589] Briefing with the Dep't of Homeland Sec. (Feb. 7, 2020).
[590] DHS00321PSI–22. In its recent response to the FCC's Show Cause Order, ComNet included a September 2014 email in which it provided Team Telecom with copies of the company's corporate charts. *See In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Response to Order to Show Cause, GN Docket No. 20-111, at Exhibit K (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=710677&f_number=ITC2142009042400199 (Email from Tammie Tam, Legal Consultant, CITIC Telecom Int'l Holdings Ltd. to Dep't of Homeland Sec. & Dep't of Justice (Sept. 3, 2014) (other senders and recipients redacted)).
[591] TT-DOJ-392–99, at TT-DOJ-398.

copies of ComNet's physical and logical technical security architecture, security policies, and IT governance controls, noting that Team Telecom was in the process of "updat[ing] [its] files."[592] After receiving the requested documents, a Team Telecom official asked to visit ComNet's offices sometime in "early-mid March . . . [to] meet with a few people to discuss on-going compliance with the [security agreement]."[593]

The requested site visit occurred on March 22, 2018.[594] According to one Team Telecom member's memo summarizing the site visit, the purpose was to, in part, "evaluate the efficacy of a [security agreement] governing the operations of a foreign state-owned company providing telecommunications services within the United States."[595] The meeting lasted two and a half hours and again focused on ComNet's "corporate structure, ownership and management, products and services, telecommunications infrastructure, security policies and procedures, procedures regarding the handling of legal process, and compliance with CALEA."[596] Among the updates provided to Team Telecom were ComNet's recent office change—from Los Angeles to West Covina, California—and its introduction of Voice over Internet Protocol ("VoIP") and basic enterprise IT services.[597]

Team Telecom concluded that ComNet was "responsive to [all] comments and questions."[598] However, Team Telecom noted:

> New services (VoIP, IT, etc.) were not contemplated when the USG parties negotiated the [security agreement] in 2009. Accordingly, the reporting requirements under the [security agreement] do little to address any new risks that may arise as ComNet expands its service offerings into new markets and grows its customer base.[599]

The Team Telecom officials attending the site visit recommended that:

> USG parties should . . . continue to monitor compliance under the [2009 security agreement] as ComNet expands its new services. This situational awareness will help inform the USG Parties [*sic*] on-going discussions concerning the [agreement's] ability to address potential

[592] *Id.* at TT-DOJ-397.
[593] *Id.* at TT-DOJ-396.
[594] *See* TT-DOJ-400–03; TT-DOJ-521–23.
[595] TT-DOJ-521–23, at TT-DOJ-521.
[596] *Id. See also* DHS00466PSI–71.
[597] TT-DOJ-521–23, at TT-DOJ-522; DHS00466PSI–71, at DHS00467PSI. ComNet reported that the revenue associated with the recently introduced services was "insignificant." At the time of the meeting, ComNet reported having only one VoIP customer. *See* TT-DOJ-521–23, at TT-DOJ-522; DHS00466PSI–71, at DHS00467PSI.
[598] TT-DOJ-521–23, at TT-DOJ-522.
[599] *Id.*

> risks to national security and law enforcement equities arising from ComNet's operations in the United States and similarly situated telecommunications companies operating pursuant to similar mitigation agreements.[600]

In July 2018, Team Telecom provided a "feedback letter" to ComNet, summarizing the March 2018 site visit.[601] Team Telecom officials and ComNet representatives informed the Subcommittee that Team Telecom has had no substantive engagement with ComNet since the site visit.[602]

5. ComNet Shares Characteristics Team Telecom Highlighted regarding China Mobile USA and CTA

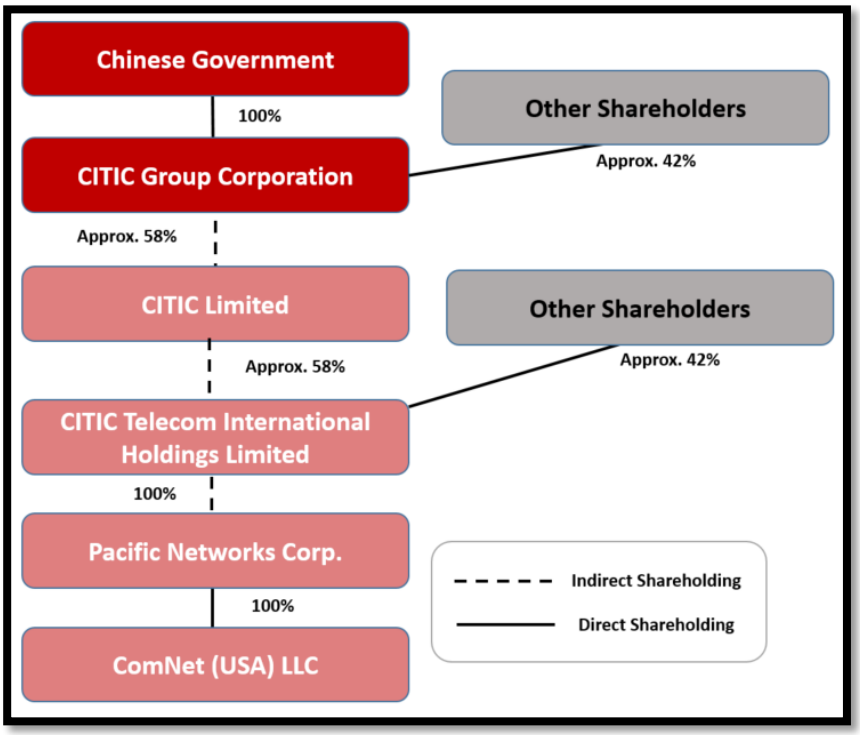
ComNet has been providing international telecommunications services pursuant to Section 214 authorizations granted over a decade ago with little oversight by the U.S. government. As described above, Team Telecom highlighted concerns about China Mobile USA's proposed and CTA's actual operations in the United States. ComNet shares similar characteristics as the other Chinese carriers.[603] It is ultimately majority-owned by the Chinese government; its parent company reviews its budget and locations in the United States; it provides a range of telecommunications services in the United States; and it has built relationships with U.S. carriers. Without proper oversight by Team Telecom, these risks have gone unmitigated.

ComNet is ultimately majority-owned by the Chinese government. As noted above, ComNet became a wholly-owned subsidiary of Pacific Networks as part of its acquisition by CITIC. CITIC is majority-owned by CITIC Group Corporation ("CITIC Group"),[604] "a wholly state-owned company in the [People's Republic of China]."[605] According to CITIC's website, CITIC Group was "established in 1979 . . . with the support of late Chinese leader Deng Xiaoping" and "since its inception, CITIC Group has been a pilot for national economic reform and an

---

[600] *Id.* at TT-DOJ-522–23.
[601] TT-DOJ-481–83.
[602] *See* Email from the Dep't of Homeland Sec. to the Subcommittee (Feb. 14, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[603] In discussions with the Subcommittee and in its response to the FCC's Order to Show Cause, ComNet distinguished its operations from China Mobile USA and CTA. According to ComNet, the companies differ in terms of company size, scope of business operations, corporate ownership structure, history of operations in the United States, and employment of U.S. citizens. *See* Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee); *In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Response to Order to Show Cause, GN Docket No. 20-111, at 19–26 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=710677&f_number=ITC2142009042400199.
[604] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee).
[605] CITIC TELECOM INTERNATIONAL, ANNUAL REPORT 248 (2019), https://www.citictel.com/wp-content/uploads/2020/03/EW01883_AR_20200327.pdf.

important window on China's opening to the outside world."[606] The diagram below depicts the relevant ownership structure:



[607]

CITIC reviews ComNet's budget and U.S. locations and may be able to access U.S. customer records. During the 2014 site visit, ComNet representatives told Team Telecom officials that the Chinese government's ownership in ComNet was passive and that it provided no input into the company's operational decisions.[608] ComNet representatives similarly informed the Subcommittee that its daily operations are managed by its local management team in California.[609] The representatives, however, acknowledged that CITIC reviews the company's budget and U.S. locations.[610] CITIC also guides ComNet on its information security

---

[606] *Major Shareholder – About CITIC Group*, CITIC TELECOM INTERNATIONAL, https://www.citictel.com/about-us/major-shareholder/.
[607] The diagram is derived from information ComNet provided to the Subcommittee, as well as publicly available information. *See Major Shareholder – About CITIC Group*, CITIC TELECOM INTERNATIONAL, https://www.citictel.com/about-us/major-shareholder/; CITIC TELECOM INTERNATIONAL, ANNUAL REPORT 99, 250 (2019), https://www.citictel.com/wp-content/uploads/2020/03/EW01883_AR_20200327.pdf; ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); *In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Response to Order to Show Cause, GN Docket No. 20-111, at Exhibit A (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=710677&f_number=ITC2142009042400199.
[608] DHS00460PSI–65, at DHS00462PSI.
[609] Briefing with ComNet (Apr. 13, 2020).
[610] *Id.*

policies.[611] ComNet maintains a company-specific policy, but that policy was drafted based on CITIC's guidance.[612]

ComNet leverages CITIC's network operations center ("NOC"), located in Hong Kong, for "first tier monitoring" against cyber incidents or disruptions.[613] "All system alarms and network management data are sent to the NOC . . . ."[614] Further, CITIC's NOC maintains records of all alarms and access logs generated by ComNet's systems.[615]

ComNet representatives informed the Subcommittee that its data center and all backed-up information are located in the United States and that it controls access to all U.S. records and data systems.[616] However, records of Team Telecom's site visits indicate that ComNet used CITIC's data center in Hong Kong as a backup and that ComNet's wholesale billing records "are maintained in Hong Kong."[617] Team Telecom's records from the 2018 site visit also note that ComNet's VoIP customer and billing records are accessible to Hong Kong personnel.[618] ComNet informed the Subcommittee, by contrast, that its parent companies do not have direct access to these records and that they would need to request access from ComNet and follow ComNet's local procedures.[619]

ComNet provides various communications services in the United States with its Section 214 authorizations. ComNet provides international telecommunication services, consisting of wholesale direct dial services, wholesale SMS services, retail prepaid calling card services, and VoIP services.[620] Pacific Networks primarily provides international resold data services.[621] Together, the companies serve a mix of carrier customers, individual end-customers, and enterprise customers in the United States.[622]

---

[611] *Id.*
[612] *Id.*
[613] *Id.*
[614] DHS00460PSI–65, at DHS00462PSI.
[615] *Id.*
[616] Briefing with ComNet (Apr. 13, 2020).
[617] DHS00460PSI–65, at DHS00463PSI; DHS00466–71, at DHS00468PSI.
[618] DHS00466–71, at DHS00470PSI.
[619] *See* Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[620] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); DHS00462PSI, DHS00467PSI.
[621] DHS00462PSI.
[622] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).

Through its wholesale international direct dial services, ComNet handles inbound and outbound voice traffic for U.S. carrier customers.[623] International voice traffic is routed through ComNet's global MPLS network.[624] Thus, ComNet uses a routing approach that allows data to be directed from one node to the next based on routing labels.[625] Data is aggregated on its voice communications platform, which is located at ComNet's point of presence in Los Angeles.[626] From there, data is transmitted to the end-user through either an internet connection provided by Cogent or through a time-division multiplexing ("TDM") connection operated by U.S. carriers.[627] According to ComNet representatives, customers select which TDM vendor ComNet uses to route communications.[628] ComNet also provides SMS services to U.S. carrier customers. Unlike the voice communications platform housed at ComNet's Los Angeles facility, however, SMS communications are aggregated on CITIC's SMS hub platform in Hong Kong.[629] Thus, all international SMS communications are routed through CITIC's servers.[630]

ComNet's retail calling cards are targeted towards end-users in the United States.[631] The calls are routed in a similar manner as international voice calls, but customers in the United States must dial local access numbers.[632] ComNet obtains these numbers from major U.S. carriers.[633]

In 2017, ComNet began offering VoIP services to business customers.[634] These services allow office users the functions of an office telephone system.[635] Through VoIP phones provided either by ComNet or by the business itself, users

---

[623] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[624] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[625] *Multiprotocol Label Switching*, TECH TARGET, https://searchnetworking.techtarget.com/definition/Multiprotocol-Label-Switching-MPLS.
[626] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[627] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020); DHS00466–71, at DHS00468PSI. The TDM connection is a physical fiber line that connects two points. Briefing with ComNet (Apr. 13, 2020).
[628] Briefing with ComNet (Apr. 13, 2020).
[629] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[630] *Cf.* Briefing with ComNet (Apr. 13, 2020).
[631] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[632] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[633] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020); Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[634] DHS00466–71, at DHS00468PSI; TT-DOJ-521–23, at TT-DOJ-522.
[635] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); DHS00466–71, at DHS00468PSI.

can make both domestic and international calls through ComNet's voice services platform.[636] According to Team Telecom, incoming VoIP calls are delivered to end-customers through 7G Network.[637] Team Telecom's records also indicate that ComNet provided basic enterprise IT services, such as video conferencing and website and software development.[638] Team Telecom flagged that these services were not contemplated at the time the security agreement was entered into and thus, the existing reporting requirements did little to address the associated risks.[639]

Unlike the other carriers discussed above, ComNet has only one point of presence in the United States, located in Los Angeles, California.[640] Team Telecom records describe the Los Angeles facility as "the premier communications hub of the Pacific Rim and arguably the single most important point of connectivity in the Western United States."[641] ComNet's servers, equipment, and data center are all housed at the Los Angeles facility, including the servers that support its various services and a billing server.[642]

ComNet has built relationships with major U.S. carriers. Like the other Chinese carriers, ComNet does not own transmission networks in the United States. It leases network capacity and equipment from major U.S. carriers to transport data from the Los Angeles facility to its end customers.[643] ComNet has established relationships with Verizon and CenturyLink, among other U.S. carriers.[644] Verizon maintains an interconnection agreement with ComNet and leases customer premise equipment, Ethernet private lines, general internet access, and private IP access.[645] Although not providing specifics, CenturyLink indicated that it had some limited commercial relationships with ComNet related to providing

---

[636] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); DHS00466–71, at DHS00468PSI.
[637] DHS00466–71, at DHS00468PSI. 7G Network is a U.S.-based telecommunications company. *About—7G Network, Inc.*, LINKEDIN, https://www.linkedin.com/company/7g-network-inc-/about/.
[638] DHS00466–71, at DHS00467PSI; TT-DOJ-521–23, at TT-DOJ-522.
[639] TT-DOJ-521–23, at TT-DOJ-522.
[640] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee).
[641] DHS00460PSI–65, at DHS00463PSI; DHS00466–71, at DHS00468PSI.
[642] ComNet Presentation to the Subcommittee (Apr. 13, 2020) (on file with the Subcommittee); Briefing with ComNet (Apr. 13, 2020).
[643] *See generally* DHS00460PSI–65; TT-DOJ-521–23.
[644] Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019). As noted above, in addition to voice and data termination services, ComNet obtains local access numbers needed for its retail calling card services from local carriers. Briefing with ComNet (Apr. 13, 2020); Letter from Lerman Senter PLLC, counsel to ComNet, to the Subcommittee (June 2, 2020) (on file with the Subcommittee). Unlike its relationships with CTA and CUA, AT&T's relationship with ComNet is limited to providing ComNet retail telephone and TV services for its own consumption. *See* Email from Gibson, Dunn & Crutcher LLP, counsel to AT&T, to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[645] Briefing with Verizon (Sept. 4, 2019).

network services, circuits, or collocation services.[646] As with CTA and CUA, neither Verizon nor CenturyLink maintains any mitigation or other agreement focused on network security with ComNet under their current arrangements.[647] The U.S. carriers do, however, employ security measures that apply regardless of whether an interconnection agreement exists.[648]

* * * * *

On April 24, 2020, the FCC issued an order requiring ComNet (and Pacific Networks) to demonstrate why its Section 214 authorizations should not be revoked.[649] The companies jointly responded to the order on June 1, 2020.[650] The companies stressed that they have successful business records and have complied fully with FCC regulatory requirements and Team Telecom requests.[651] Further, the companies stated that they have never been "asked by the Chinese government or the Chinese Communist Party to take any action that would 'jeopardize the national security and law enforcement interests of the United States' or would suggest that the Companies are vulnerable 'to the exploitation, influence, and control of the Chinese government.'"[652] As with CUA, ComNet and Pacific Networks noted that the federal government has not highlighted any activity taken by either company that might endanger national security, aside from being "ultimately owned by public companies with partial Chinese state ownership."[653] The companies distinguished their licensing history from that of China Mobile USA.[654] ComNet and Pacific Networks concluded their response by noting, although revocation is not warranted, should additional mitigation be deemed necessary, they are open to discussing appropriate conditions with the FCC or Team Telecom.[655] The FCC is evaluating the information ComNet and Pacific Networks submitted and considering whether to revoke their authorizations.

---

[646] Briefing with CenturyLink (Sept. 10, 2019).
[647] *See* Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019). According to Verizon, its agreements are consistent with those it has with other carriers. Teleconference with Verizon (June 2, 2020).
[648] *See* Briefing with Verizon (Sept. 4, 2019); Briefing with CenturyLink (Sept. 10, 2019); Teleconference with Verizon (June 2, 2020); Email from CenturyLink to the Subcommittee (June 2, 2020) (on file with the Subcommittee).
[649] *See In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Order to Show Cause, DA 20-450 (Apr. 24, 2020), https://docs.fcc.gov/public/attachments/DA-20-450A1.pdf.
[650] *In the Matter of Pacific Networks Corp. and ComNet (USA) LLC*, Response to Order to Show Cause, GN Docket No. 20-111 (June 1, 2020), http://licensing.fcc.gov/cgi-bin/ws.exe/prod/ib/forms/reports/related_filing.hts?f_key=710677&f_number=ITC2142009042400199.
[651] *Id.* at i, 2, 20.
[652] *Id.* at i–ii, 2, 19.
[653] *Id.* at 2.
[654] *Id.* at 22–23.
[655] *Id.* at 31–32.

VI. CONCLUSION

It is well understood that the national security environment evolves over time. It is this constant evolution that highlights a major flaw with the FCC's Section 214 authorizations: once authorized, a company can operate indefinitely without any oversight. Without proper oversight, foreign carriers operating in the United States can expose the United States to potential economic, national security, and law enforcement risks. The federal government has highlighted the potential risks associated with Chinese telecommunications carriers operating in the United States. Three particular carriers have been operating in the United States for approximately 20 years, without sufficient oversight from the FCC and the Executive Branch. Especially when dealing with state-owned telecommunications carriers, greater controls are needed, and the Administration and Congress must work together to ensure sufficient safeguards and oversight mechanisms are in place.