

Executive Branch Recommendation to the Federal Communications Commission to Deny China Mobile International (USA) Inc.'s Application for an International Section 214 Authorization

The Executive Branch¹ recommends that the Federal Communications Commission (FCC or Commission) deny the application of China Mobile International (USA) Inc. (China Mobile) for a certificate of public convenience and necessity under Section 214 of the Communications Act, as amended, 47 U.S.C. § 214(a) (ITC-214-20110901-00289). This application raises substantial and unacceptable national security and law enforcement risks in the current national security environment. These risks cannot be resolved through a voluntary mitigation agreement, as China Mobile has proposed. Therefore, it is the view of the Executive Branch that the application does not serve the public interest.

The basis for the Executive Branch's recommendation is set forth in the discussion below. The Executive Branch is also submitting a classified appendix describing additional information relevant to China Mobile's application.

1. Summary of recommendation for denial of application

In September 2011, China Mobile applied to the FCC for authorization under Section 214 of the Communications Act of 1934,² in order to offer telecommunications services as a common carrier between the United States and international locations. Although China Mobile is incorporated in Delaware, its majority owner is China Mobile Hong Kong (BVI) Limited, which is wholly owned by China Mobile Communications Corporation, which in turn is wholly owned by a foreign state, the People's Republic of China, and is subject to the supervision of the State-Owned Assets Supervision and Administration Commission (SASAC) of the State Council of the People's Republic of China. China Mobile has acknowledged in its international Section 214 authorization application that it is indirectly owned – 74.2 percent at the time of filing with the FCC – by the Chinese government.³

Pursuant to Section 214 of the Communications Act, an applicant may not provide international “common carrier” services without obtaining a Section 214 authorization from the FCC. The FCC may only issue such an authorization if “the present or future public convenience and necessity require or will require the

¹ The Executive Branch includes the Departments of Justice, Homeland Security, Defense, State, and Commerce, as well as the Offices of Science and Technology Policy and the United States Trade Representative (collectively, the Executive Branch or Executive Branch Agencies).

² 47 U.S.C. § 214(a).

³ See ITC-214-20110901-00289 e-file.

construction, or operation, or construction and operation,” of the telecommunications lines the application seeks to operate.⁴ The FCC has the authority to issue, refuse to issue, issue in part, or issue with conditions such an authorization.⁵ As the FCC has explained, “[t]he *Applicants* bear the burden of proving, by a preponderance of the evidence, that the proposed transaction, on balance, will serve the public interest.”⁶

Because the FCC has recognized that foreign investment in U.S. telecommunications carriers may implicate issues uniquely within the expertise of the Executive Branch, when an applicant reports a foreign individual or entity with 10 percent or greater ownership in the applicant, the FCC routinely seeks the views of various components of the Executive Branch as to whether the pending application poses any “national security, law enforcement, foreign policy or trade concerns.”⁷ Section 214 requires the FCC to notify the Secretary of Defense of an application, and for applications involving service to foreign points, to notify the Secretary of State, among others.⁸ The FCC relies on the expertise of the Executive Branch Agencies to identify and evaluate—and when appropriate, to reduce and manage—those concerns. The FCC “accord[s] deference to [Executive Branch] expertise . . . in identifying and interpreting issues of concern related to national security, law enforcement, and foreign policy that are relevant to an application pending before [it].”⁹ The FCC, consistent with this long-standing practice when an applicant reports a 10 percent or greater foreign ownership, has asked whether the Executive Branch Agencies have such concerns arising out of China Mobile’s application.

The Executive Branch strongly supports the policy of the FCC to promote robust foreign participation in the U.S. telecommunications market. The additional capital, technology, and competition associated with the openness of the U.S. telecommunications market benefits American consumers and businesses alike. Indeed, for well over two decades, the U.S. market has been one of the largest destinations of foreign investment in telecommunications. Further, the openness of the U.S. market has enabled the United States to seek comparable market access in other markets in a credible manner, which also benefits U.S. consumers and businesses. However, the deepening integration of the global telecommunications market has created risks and vulnerabilities

⁴ 47 U.S.C. § 214(a); *see also* 47 CFR § 63.18.

⁵ 47 U.S.C. § 214(a), (c).

⁶ *In re Applications of Cellco P’ship d/b/a Verizon Wireless and Atlantis Holdings LLC*, 23 FCC Rcd 17444, 17460–61 ¶ 26 (2008) (emphasis added); *see also* 47 CFR § 63.18.

⁷ *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market: Market Entry and Regulation of Foreign-Affiliated Entities*, IB Docket Nos. 97-142 and 95-22, Report and Order and Order on Reconsideration, FCC 97-398, 12 FCC Rcd 23891 (1997) (*Foreign Participation Order*), Order on Reconsideration, FCC 00-339, 15 FCC Rcd 18158, 23891, 23919 (2000).

⁸ *See* 47 U.S.C. § 214(b).

⁹ *Foreign Participation Order*, 12 FCC Rcd at 23920 ¶ 63.

in a sector replete with a broad range of malicious activities. Accordingly, the Executive Branch acts to establish the necessary balance between maintaining an open investment policy and protecting our national security and law enforcement requirements. In the current national security environment, it is the view of the Executive Branch, after consultation with the U.S. intelligence community, and after consideration of additional information submitted by the applicant, that China Mobile's application does not serve the public interest. To the contrary, the authorization would pose substantial, unacceptable national security and law enforcement risks. Thus, the Executive Branch recommends that the FCC deny China Mobile's application in order to protect the national security and law enforcement interests of the United States. Although China Mobile has proposed voluntary mitigation measures, the Executive Branch believes that the substantial national security and law enforcement risks that have been identified with respect to China Mobile cannot be resolved through any of these mitigation measures or others that it has considered.

2. China Mobile's international Section 214 authorization application and planned activities

When China Mobile filed its application with the FCC for an international Section 214 authorization in 2011, its parent company, the China-based China Mobile Communications Corporation, was the world's largest mobile phone operator with more than 649 million subscribers and approximately 164,000 employees. China Mobile Communications Corporation is a Chinese state-owned enterprise subject to the supervision of a Chinese government body, the SASAC. As noted above, China Mobile Communications Corporation owns more than 70 percent of China Mobile. Although China Mobile has stated that SASAC does not directly participate in its management and operations,¹⁰ China Mobile has not contended that it is not subject to SASAC supervision.

China Mobile's acquisition of an international Section 214 authorization would render it a "common carrier" under federal law, thereby enabling it to carry international voice traffic between the United States and foreign countries, and to interconnect such traffic with the U.S. telecommunications network. Subject to the requirements of the Communications Act, telecommunications carriers can enter into a full range of direct and indirect interconnection relationships with other telecommunications carriers, from basic connections between networks in order to exchange traffic (so that a customer of carrier A can call a customer of carrier B) to much more integrated relationships (in which carrier A may have greater access to certain of carrier B's network elements and cell sites).

¹⁰ Response from China Mobile to Executive Branch Agency's October 5, 2011 questions (Nov. 3, 2011) [Exhibits 1, 2].

Section 201 of the Communications Act states that:

It shall be the duty of every common carrier engaged in interstate or foreign communications by wire or radio to furnish such communication service upon reasonable request therefor; and, in accordance with the orders of the Commission, in cases where the Commission, after opportunity for hearing, finds such action necessary or desirable in the public interest, to establish physical connections with other carriers, to establish through routes and charges applicable thereto and the divisions of such charges, and to establish and provide facilities and regulations for operating such through routes.¹¹

This establishes at least basic interconnection between carriers to handle the exchange of traffic. In addition, pursuant to the Communications Act and the Commission's regulations, all telecommunications carriers are subject to a general duty to "interconnect directly or indirectly with the facilities and equipment of other telecommunications carriers."¹² Securing an international Section 214 authorization would allow China Mobile to enter such interconnection relationships with domestic telecommunications carriers and their networks; indeed, domestic carriers are required to enter these relationships pursuant to the Communications Act.

Since China Mobile filed its international Section 214 authorization application with the FCC, individual components of the Executive Branch have engaged with China Mobile on numerous occasions to learn more about its management, business, and proposed activities. China Mobile responded to a series of questions regarding its business and planned operations, on multiple occasions from 2011 to 2012. Should it obtain an international Section 214 authorization, China Mobile has stated that it intends to [[REDACTED]].¹³ China Mobile has stated that it does not intend to offer domestic telephone services within the United States.¹⁴ China Mobile has also stated that it does not plan to offer mobile services in the United States.¹⁵ In anticipation of offering international voice traffic between the United States and foreign countries, China Mobile has also informed the Executive Branch that [[REDACTED]]

¹¹ 47 U.S.C. § 201(a).

¹² 47 U.S.C. § 251(a)(1); 47 CFR § 51.100(a)(1).

¹³ Response from China Mobile to Executive Branch Agency's October 5, 2011 questions (Nov. 3, 2011) [Exhibits 1, 2].

¹⁴ Response from China Mobile to Executive Branch Agency's February 28, 2012 questions (Apr. 27, 2012) [Exhibits 3, 4].

¹⁵ *Id.*

[[REDACTED]]
[[REDACTED]].¹⁶ [[REDACTED]], China Mobile [[REDACTED]]
[[REDACTED]]
[[REDACTED]].¹⁷ As of 2012, China Mobile had [[REDACTED]]
[[REDACTED]]
[[REDACTED]] in order to offer its planned services upon acquiring an international Section 214 authorization. For example, China Mobile discussed [[REDACTED]]
[[REDACTED]]
[[REDACTED]].¹⁸

In the fall of 2014, China Mobile provided the FCC and certain Executive Branch Agencies with additional information about its business and the types of services it intends to offer. In September 2014, in response to questions posed by the Executive Branch, China Mobile [[REDACTED]]
[[REDACTED]]
[[REDACTED]].¹⁹ China Mobile also informed the Executive Branch that [[REDACTED]]
[[REDACTED]].²⁰ In October 2014, China Mobile indicated that, [[REDACTED]]
[[REDACTED]]
[[REDACTED]]. China Mobile noted that [[REDACTED]]
[[REDACTED]].²¹ China Mobile also noted that [[REDACTED]]
[[REDACTED]]
[[REDACTED]].²²

China Mobile has also requested more information about the Executive Branch review process and reasons why the review process is still ongoing. On May 14, 2015, in the interest of transparency and with the goal of facilitating dialogue with China Mobile, the Executive Branch sent China Mobile a letter outlining the kinds of considerations that

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ Letter from Kent Bressie, counsel to China Mobile, to U.S. Dep't of Justice (Sept. 25, 2014) [Exhibit 6]. China Mobile [[REDACTED]]
[[REDACTED]].

²¹ Presentation from China Mobile to the U.S. Dep't of State (Oct. 31, 2014) [Exhibit 7].

²² Response from China Mobile to Executive Branch Agency's October 5, 2011 questions (Nov. 3, 2011) [Exhibits 1, 2].

the Executive Branch weighs when evaluating international Section 214 authorization applications and invited China Mobile to use the information when developing proposed mitigation measures. The letter informed China Mobile that the Executive Branch would consider a range of factors in the context of the current national security environment, including, but not necessarily limited to:

- **The Applicant:** Whether the applicant has a past criminal history; whether the applicant has engaged in conduct that calls the applicant's trustworthiness into question; and whether the applicant 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 or an entity controlled by or acting on behalf of a foreign government; whether the applicant's foreign ownership is from a country suspected of engaging in actions, or possessing the intention to take actions, that could impair U.S. national security; whether the applicant will be required, by virtue of its foreign ownership, to comply with foreign requests (e.g., requests for communications intercepts) relating to the applicant's operations within the United States, or whether the applicant is otherwise susceptible to such requests and/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) 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. This consideration includes an evaluation as to

the continued efficacy of confidentiality requirements that protect information about the targets of lawful surveillance and classified sources and methods.²³

That notification represented the first time the Executive Branch has provided a written statement to an international Section 214 authorization applicant describing the factors it considers in determining whether an application presents national security and law enforcement concerns. The factors themselves, however, are not new, and the Executive Branch has routinely weighed such factors when evaluating past international Section 214 authorization applications. The Executive Branch developed these factors based on input from agencies responsible for law enforcement and national security matters, as well as past experience evaluating FCC authorization applications and monitoring the effectiveness of mitigation measures. In a June 12, 2015 response, China Mobile sent the Executive Branch the proposed mitigation measures discussed below in Part 3.3.

3. Granting China Mobile's international authorization application would not be in the public interest in the current national security environment

The Executive Branch considered China Mobile's application, as well as its proposed mitigation measures, in light of these factors and concluded that, because China Mobile is subject to exploitation, influence, and control by the Chinese government, granting China Mobile's international Section 214 application, in the current national security environment, would pose substantial and unacceptable national security and law enforcement risks. These risks, moreover, in the current national security environment, and in light of China Mobile's anticipated operations involving interconnection with the U.S. telecommunications infrastructure and the importance and sensitivity of that infrastructure to U.S. national security and law enforcement interests, cannot adequately be resolved through a mitigation agreement between China Mobile and the Executive Branch, for reasons discussed in part 3.3 below. Therefore, it is the view of the Executive Branch that granting China Mobile's international Section 214 application is not in the public interest.

3.1. China Mobile is subject to exploitation, influence, and control by the Chinese government

As communicated to China Mobile in the May 14, 2015 letter sent by the U.S. Department of Justice, one of the factors the agencies consider in evaluating an international Section 214 authorization application is whether the applicant is vulnerable to exploitation, influence, and control by other actors – including whether an applicant's foreign ownership could result in the control of U.S. telecommunications infrastructure or persons operating such infrastructure by a foreign government or an entity controlled by

²³ Letter from U.S. Dep't of Justice to China Mobile (May 14, 2015) [Exhibit 9].

or acting on behalf of a foreign government. In a response dated June 12, 2015, China Mobile stated that it would not be required, by virtue of its foreign ownership, to comply with foreign requests relating to its operations within the United States. China Mobile also stated that it is no more vulnerable to exploitation, influence, or control by other actors than any other U.S. or foreign carrier that uses what China Mobile characterized as “best-practice” measures to guard against such risk.²⁴

However, the Executive Branch has assessed that China Mobile is vulnerable to exploitation, influence, and control by the Chinese government and that China Mobile would likely comply with requests made by the Chinese government. Although state ownership or control does not, standing alone, necessarily pose a threat to U.S. national security and law enforcement interests, for the reasons stated below, the Executive Branch believes that granting the authorization poses an unacceptable risk to U.S. national security and law enforcement, and that the risk can be expected to increase over time. This assessment rests in large part on China’s record of intelligence activities and economic espionage targeting the United States, along with China Mobile’s size and technical and financial resources.

China Mobile Communications Company – and by extension, its subsidiary China Mobile – as a prominent Chinese state-owned enterprise, cannot be expected to act against the interest of the Chinese government on any sensitive matter. Certainly at a minimum, China Mobile would be expected to comply with any requests or orders for assistance from the Chinese government, including its security services.

As a result, the Executive Branch believes that China Mobile would likely comply with requests by the Chinese government for information, access to its network, and any other assistance, including activities involving cyber intrusions and attacks.

3.2. Granting China Mobile’s international Section 214 application would produce substantial and unacceptable national security and law enforcement risks

Because China Mobile is subject to exploitation, influence, and control by the Chinese government, the Executive Branch believes that granting China Mobile’s application in the context of the current national security environment would produce substantial and unacceptable national security and law enforcement risks. These risks, set out below, would likely increase over time.

In reaching this assessment, the Executive Branch has relied on its experience in national security and law enforcement and significant reporting and analysis by the Intelligence Community. The factors that gave rise to this assessment include prior

²⁴ Mitigation Proposal from China Mobile (June 12, 2015) [Exhibit 10].

Chinese government involvement in computer intrusions and attacks and economic espionage. Some of this information is contained in public documents related to criminal prosecutions,²⁵ as well as several reputable unclassified sources, including the 2014 “Report to Congress of the U.S.-China Economic and Security Review Commission” (the U.S.-China Report);²⁶ the Department of Defense 2013 report to Congress on Chinese military developments (the Defense Report);²⁷ the May 2013 report of the Commission on the Theft of American Intellectual Property (the IP Commission Report);²⁸ the Mandiant Corporation’s February 2013 study (the Mandiant Report);²⁹ and the 2012 “Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE,” by the Permanent Select Committee on Intelligence of the U.S. House of Representatives (the House Report).³⁰ In addition to the foregoing, an accompanying classified submission includes additional, more recent assessments of cybersecurity breaches and economic espionage and theft involving the Chinese government that threaten, among other things, the United States’ national security and telecommunications network infrastructure.

²⁵ See Press Release, Office of Public Affairs, U.S. Dep’t of Justice, Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors’ Systems to Steal Sensitive Military Information (Mar. 23, 2016), available at <https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive>; see also Press Release, Office of Public Affairs, U.S. Dep’t of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), available at <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

²⁶ See U.S.-China Econ. and Sec. Review Comm’n, *2014 Report to Congress of the U.S.-China Economic and Security Review Commission* (2014), available at https://www.uscc.gov/Annual_Reports/2014-annual-report-congress [hereinafter the U.S.-China Report].

²⁷ See U.S. Dep’t of Def., *Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China* (2013), available at http://archive.defense.gov/pubs/2013_China_Report_FINAL.pdf [hereinafter the Defense Report].

²⁸ See Comm’n on the Theft of Am. Intellectual Prop., *The Report of the Commission on the Theft of American Intellectual Property* (May 2013), available at http://www.ipcommission.org/report/ip_commission_report_052213.pdf [hereinafter the IP Commission Report].

²⁹ See Mandiant, *APT1: Exposing One of China’s Cyber Espionage Units* (2013), available at <https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf> [hereinafter the Mandiant Report].

³⁰ See H.R. Permanent Select Comm. on Intelligence, 112th Cong., *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE* (2012), available at [https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20\(final\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf) [hereinafter the House Report].

3.2.1. Granting China Mobile's application would present a substantial and unacceptable risk of increased Chinese government intelligence collection against U.S. targets, including economic espionage activities.

There is ample evidence that the Chinese government has engaged in extensive intelligence collection activity against the United States for national security and economic espionage purposes. As the House Report stated in 2012, Chinese intelligence collection efforts against the U.S. government at the time were growing in "scale, intensity and sophistication."³¹ The Defense Report stated in 2013 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."³²

An international Section 214 authorization would permit China Mobile to become a common carrier and thereby connect within the United States to the U.S. domestic, public-switched telephone network. A carrier connected to this network in the United States has greater access to the telephone lines, fiber-optic cables, cellular networks, and communication satellites that make up the network than an entity that does not have an international Section 214 authorization. This network was created with minimal security features because it was assumed that only trusted parties would have access. However, this lack of security features has led to law enforcement and national security vulnerabilities, such as giving an entity with access to the network the ability to target, alter, block, and re-route traffic. The Chinese government could therefore seek to use China Mobile's common carrier status to exploit the public-switched telephone network in the United States and increase intelligence collection against U.S. government agencies and other sensitive targets that depend on this network.

As a result, the Chinese government, through China Mobile, would have a greater ability to monitor, degrade, and disrupt U.S. government communications. China Mobile intends to offer its services to other carriers, which may provide telecommunications services to the U.S. government. Due to the business practice of carriers sending voice traffic over the lowest cost routes, customers are usually unaware of which carrier is handling its communications and at what point in the communication its traffic is handled by a specific carrier. Therefore, if China Mobile is granted an international Section 214 authorization, the communications of U.S. government agencies to any international destinations may pass through China Mobile's network during transit, even if the agencies are not actual China Mobile customers. Amplifying these considerations is the fact that, after obtaining an international Section 214 authorization, China Mobile could

³¹ House Report at 2 (citing U.S.-China Econ. and Sec. Review Comm'n, 2011 *Annual Report to Congress of the U.S.-China Economic and Security Review Commission* (2011)).

³² Defense Report at 36; *see also* IP Commission Report at 18.

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.³³

3.2.2. Granting China Mobile's application would present a substantial and unacceptable risk of increased economic espionage

As the Executive Branch Agencies told China Mobile in a May 2015 letter, the Agencies consider whether an applicant's planned operations within the United States provide opportunities for the applicant or other actors to engage in economic espionage against corporations that depend on the security and reliability of U.S. communications infrastructure to engage in lawful business activities. The Executive Branch assesses that China Mobile's possession of an international Section 214 authorization would increase the vulnerability of firms doing business in the United States to Chinese economic espionage.

Chinese economic and cyber espionage against targets in the United States, including espionage conducted by Chinese government actors, has been extensive. As the House Report noted, Chinese actors are "the world's most active and persistent perpetrators of economic espionage."³⁴ The U.S.-China Report stated that "China's cyber espionage continued unabated in 2014, despite a concerted U.S. effort since 2013 to expose and stigmatize Chinese economic espionage."³⁵ The IP Commission Report also cited the Mandiant Report, which traced cyberattacks on intellectual property in the United States back to Chinese government actors—specifically, the People's Liberation Army. The Mandiant Report described a Chinese People's Liberation Army cyber unit that began operations in 2006 with the purpose of accessing networks in order to commit espionage and steal data, including against U.S. firms. Mandiant concluded that this unit is fully institutionalized within the Chinese government and is able to draw upon the resources of Chinese state-owned enterprises.³⁶

³³ China Mobile stated that [[REDACTED]]. See Response from China Mobile to Executive Branch Agency's questions October 5, 2011 questions (Nov. 3, 2011) [Exhibits 1, 2].

³⁴ House Report at 2 (citing Office of Nat'l Counterintelligence Exec., *Report to Congress on Foreign Economic Collection and Industrial Espionage: Foreign Spies Stealing US Economic Secrets in Cyberspace* (2011)).

³⁵ U.S.-China Report at 34.

³⁶ See Mandiant Report at 7. See also Press Release, Office of Public Affairs, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), available at

The IP Commission Report further notes the devastating impact that Chinese state-sponsored intellectual property theft through cyber activity has had on the U.S. economy.³⁷ It cites a March 2012 report to Congress, which identified the Chinese People's Liberation Army as a key player in using computer hacking, often in concert with commercial entities, to steal intellectual property.³⁸ A Verizon study of cyber incidents, conducted in 2012 in cooperation with eighteen private organizations and government agencies, found that out of 47,000 reported intrusions, "state-affiliated actors" accounted for 19 percent of 621 successful breaches.³⁹ The Chinese government was determined to be responsible for 96 percent of cases deemed motivated by espionage.⁴⁰ Although raising the question of whether this figure was exaggerated, the IP Commission Report nonetheless concluded that the Verizon study "add[ed] weight to the findings of the other principal studies in the field, all of which point to China as the major source of state-sponsored attacks on [intellectual property]."⁴¹ According to the House Report, U.S. private-sector firms and cyber-security specialists have faced an onslaught of sophisticated computer network intrusions originating in China. The House Report presents evidence that the intrusions were almost certainly the work of the Chinese government, or were being staged with Chinese government support.

The Executive Branch's recommendation to deny China Mobile's application is consistent with a broader law enforcement and national security effort to counter malicious Chinese cyber activity against the United States. Evidence of the serious threat to the United States from Chinese cyberespionage is also reflected in the 2014 federal indictment of five Chinese military officers for cyber-theft from five corporations and a major international labor union in the United States. The indictment marked the first time criminal charges have been filed against uniformed state-actors for hacking. In announcing the charges, the Director of the Federal Bureau of Investigation stated, "[f]or too long, the Chinese government has blatantly sought to use cyber espionage to obtain economic advantage for its state-owned industries."⁴² In 2015, the presidents of the United States and China committed that neither government would conduct or knowingly

<https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

³⁷ See IP Commission Report at 43.

³⁸ See *id.* at 18 (citing Brian Krekel et al., Northrop Grumman Corp., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* at 13 (2012)).

³⁹ See *id.* (citing Verizon, RISK Team, *2013 Data Breach Investigations Report* at 4-5 (2013)).

⁴⁰ See *id.*

⁴¹ *Id.*

⁴² Press Release, Office of Public Affairs, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), available at <https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor>.

support computer intrusions or attacks for the purposes of stealing intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.⁴³ Despite this commitment, businesses operating in the United States continue to experience computer intrusions and attacks that focus on the theft of intellectual property and are connected to individuals and entities in China.⁴⁴ As the U.S. Trade Representative's 2018 Section 301 findings into China's acts and policies related to technology transfer and intellectual property declares, "[s]tate-sponsored cyber intrusions originating from China into U.S. commercial networks occur alongside China's institutional framework for promoting its industrial technological development through a state-led model in which state-owned enterprises and national champions are the recipient of extensive state support."⁴⁵

3.2.3. Granting China Mobile's application would present a substantial and unacceptable risk to U.S. law enforcement and foreign intelligence collection

As communicated by the Executive Branch to China Mobile, the Executive Branch considers whether it will be able to continue to conduct its statutorily authorized law enforcement and national security missions in evaluating an international Section 214 authorization application. These missions require serving legal process for the production of information and the provision of technical assistance. The Executive Branch must evaluate the continued efficacy of confidentiality requirements that protect information about the targets of such lawful surveillance and classified sources and methods.

The U.S. government would not be able to work effectively with China Mobile to identify and disrupt unlawful activities such as computer intrusions, or to assist in the investigation of past and current unlawful conduct, as the U.S. government does with trusted voice communication providers. These efforts rely on a baseline level of trust between the government and telecommunications carriers. In particular, the carriers must be willing to share accurate information with the U.S. government and to cooperate fully in investigations. The government must be able to trust that the information it provides to the carriers will be kept in confidence and used by the carrier solely for the purpose of protecting its network. In addition to the reasons outlined above, and in part because

⁴³ See Press Release, Office of the Press Sec'y, White House, Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference (Sept. 25, 2015).

⁴⁴ Press Release, Office of Public Affairs, U.S. Dep't of Justice, U.S. Charges Three Chinese Hackers Who Work at Internet Security firm for Hacking Three Corporations for Commercial Advantage (November 27, 2017), available at <https://www.justice.gov/opa/pr/us-charges-three-chinese-hackers-who-work-internet-security-firm-hacking-three-corporations>.

⁴⁵ Office of U.S. Trade Rep., *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, at 170 (Mar. 22, 2018).

China Mobile is majority-owned by the Chinese government, which the Executive Branch assigns responsibility for a significant amount of unlawful activity, including many cyber intrusions against the United States, China Mobile cannot serve as a trusted voice communication provider for these purposes. The Executive Branch believes that the United States will be unable to rely on China Mobile's assistance in preventing such intrusions or in identifying and holding accountable those responsible.

3.2.4. The national security and law enforcement risks have evolved since the FCC last granted a large Chinese state-owned enterprise's Section 214 application

China Mobile's authorization application should be denied, despite the fact that the FCC has granted international Section 214 authorizations to other Chinese state-owned companies in the past. Although the Executive Branch did not recommend denying those prior authorizations, the national security environment has changed as the sophistication and resulting damage of the Chinese government's involvement in computer intrusions and attacks against the United States has evolved over time. These developments in the national security environment are relevant to the Executive Branch's current assessment. As a consequence, the Executive Branch has assessed that the risks associated with granting an international Section 214 authorization to China Mobile are different and heightened. Moreover, China Mobile raises special concerns due to its size and technical and financial resources. The Executive Branch has increased knowledge of the risks of granting international Section 214 authorizations to Chinese state-owned carriers, including increased awareness of China's role in economic and other espionage against the United States. As a result, prior mitigation measures applied to certain Chinese state-owned companies would be insufficient here to address the risks posed by granting an international Section 214 authorization to China Mobile in an adequate manner.

3.3. The substantial and unacceptable national security and law enforcement risks cannot be resolved through a mitigation agreement in the current national security environment

The Executive Branch's evaluation of China Mobile's application has included both a careful review of mitigation approaches suggested by China Mobile as well as consideration of other potential mitigation approaches independently identified by the Executive Branch in an effort to examine fully all potential mitigation options. At the request of the Executive Branch, China Mobile provided significant information about its business and planned services. This information, as well as the mitigation proposals offered by China Mobile, were carefully considered, analyzed, and discussed within the Executive Branch over the course of dozens of meetings. The Executive Branch also evaluated various other mitigation options. Much of this consideration focused on











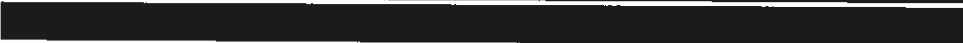
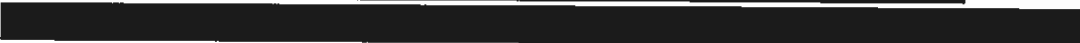






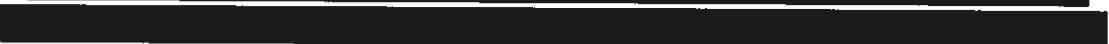
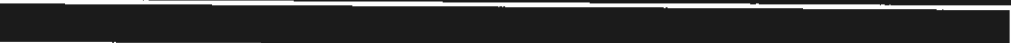



technical implications of the authorization being granted and whether a combination of various mitigation proposals would adequately address the law enforcement and national security risks. The Executive Branch Agencies also met several times to discuss the technical feasibility of various mitigation proposals.

As a preliminary matter, China Mobile stated [[REDACTED]].⁴⁶ Although China Mobile may [[REDACTED]], it would have numerous interconnection agreements with U.S. carriers. China Mobile has stated [[REDACTED]]

]].⁴⁷ Given these planned interconnection arrangements – as well as connections to China Mobile’s anticipated customers, including fixed and mobile network operators, wholesale carriers, calling card companies, phone line companies, and enterprise customers – the Executive Branch considers the risks described above to be unacceptable. The Chinese government could use China Mobile to conduct or to increase economic espionage and intelligence collection against the United States. Even if China Mobile [[REDACTED]], the Chinese government could still exploit China Mobile’s presence in the U.S. domestic telecommunications network and the resulting increased access to U.S. companies and data.

China Mobile has also [[REDACTED]].⁴⁸ In addition, China Mobile has informed the Executive Branch that, as required by law, it would use hardware that permits it to intercept customer communications when served with a court order and other legal process. The hardware [[REDACTED]]. So long as China Mobile controls its network, however, the security of the equipment it uses does not mitigate the risk China Mobile would pose as the operator of that equipment.⁴⁹

⁴⁶ Mitigation Proposal from China Mobile (June 12, 2015) [Exhibit 10].
⁴⁷ Response from China Mobile to Executive Branch Agency’s October 5, 2011 questions (Nov. 3, 2011) [Exhibits 1, 2].
⁴⁸ Letter from China Mobile (Oct. 7, 2013) [Exhibit 5].
⁴⁹ The Executive Branch also confirmed that China Mobile could not accept a proxy arrangement, whereby China Mobile would restrict foreign access and control to its U.S. network. See E-mail from China Mobile to the U.S. Dep’t of Def. (Jan. 28, 2015) [Exhibit 8].

The range of mitigation measures that the Executive Branch has carefully considered includes the following measures proposed by China Mobile:⁵⁰ 





















]].

It is also relevant that the understanding and experience of the Executive Branch, based among other things on an August 5, 2015 meeting with FCC staff, is that the FCC relies on the Executive Branch to monitor compliance with the specific terms it has negotiated with an applicant and that are contained in a mitigation agreement. Although the Executive Branch routinely monitors companies' compliance with their mitigation agreements on an ongoing basis, the Executive Branch can never have full visibility into all of a company's activities. Therefore, the Executive Branch necessarily relies on the other party to adhere rigorously and scrupulously to mitigation agreement provisions, and to self-report any problems or issues of non-compliance. However, because China Mobile is subject to exploitation, influence, and control by the Chinese government, as discussed above in Section 3.1, the Executive Branch believes that China Mobile could at the behest of the Chinese government violate the mitigation agreement and not self-report, as it may be required to do so under Chinese law. The Executive Branch further notes that even if any breaches were promptly discovered and resolved, the potential

⁵⁰ Mitigation Proposal from China Mobile (June 12, 2015) [Exhibit 10].

harms could very likely not be remediated. For example, disclosure to the Chinese government of national security or law enforcement requests or the unauthorized access to customer or company data could create irreparable damage to U.S. national security, and it would be impossible to unring the bell and bring the company back into compliance.

For all of these reasons, and after careful consideration, the Executive Branch ultimately determined that no combination of mitigation measures would adequately address law enforcement and national security concerns in the current national security environment.

4. Conclusion

For the reasons set forth above, the Executive Branch recommends that the FCC deny the application of China Mobile for a certificate of public convenience and necessity under Section 214 of the Communications Act, as amended, 47 U.S.C. § 214(a) (ITC-214-20110901-00289).

The Executive Branch believes that the above unclassified information is independently sufficient to justify this recommendation. However, the attached appendix provides additional classified information to support further our recommendation to deny China Mobile's application.

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.’s Application for an International
Section 214 Authorization**

EXHIBITS

- 1, 2 Response from China Mobile to Executive Branch Agency’s October 5, 2011 questions (Nov. 3, 2011)
- 3, 4 Response from China Mobile to Executive Branch Agency’s February 28, 2012 questions (Apr. 27, 2012)
- 5 Letter from China Mobile (Oct. 7, 2013)
- 6 Letter from Kent Bressie, counsel to China Mobile, to U.S. Dep’t of Justice (Sept. 25, 2014)
- 7 Presentation from China Mobile to the U.S. Dep’t of State (Oct. 31, 2014)
- 8 E-mail from China Mobile to the U.S. Dep’t of Def. (Jan. 28, 2015)
- 9 Letter from U.S. Dep’t of Justice to China Mobile (May 14, 2015)
- 10 Mitigation Proposal from China Mobile (June 12, 2015)

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 1

WILKINSON) BARKER) KNAUER) LLP

2300 N STREET, NW
SUITE 700
WASHINGTON, DC 20037
TEL 202.783.4141
FAX 202.783.5851
WWW.WBKLaw.COM
JENNIFER L. KOSTYU
DIRECT 202.383.3384
JKOSTYU@WBKLAW.COM

November 3, 2011

VIA EMAIL:

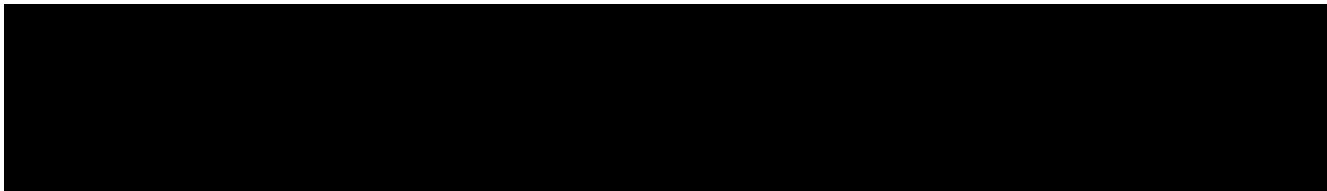


Team Telecom
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Attn: Marilyn Shaifer and Tyrone Brown

Re: *Responses of China Mobile International (USA) Inc. to Team Telecom
Inquiry and Request for Confidential Treatment
FCC File No. ITC-214-20110901-00289*

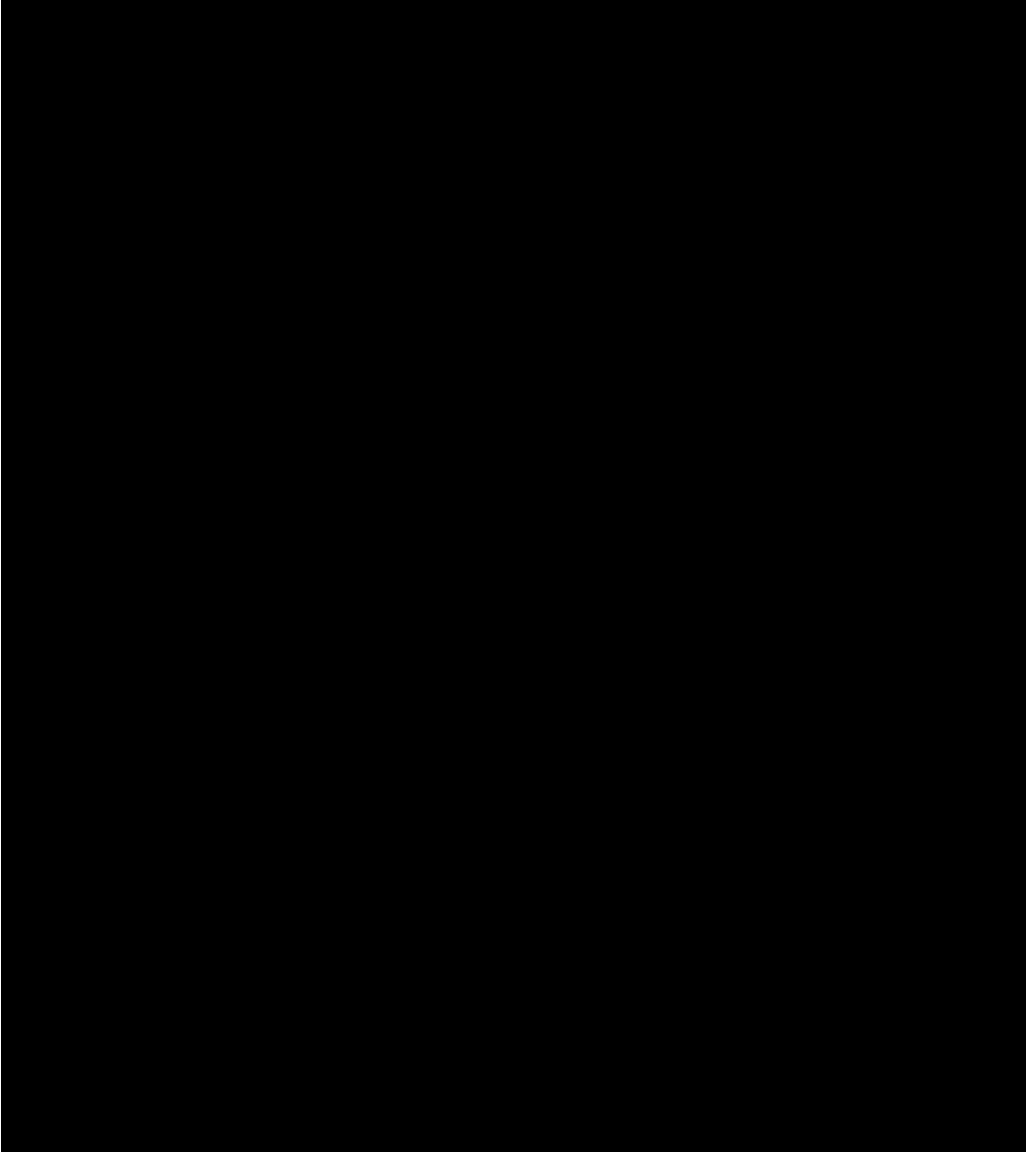
Dear Ms. Shaifer and Mr. Brown:

Enclosed please find the response of China Mobile International (USA) Inc. (“China Mobile USA” or the “Applicant”) to your October 5, 2011 questions relating to the above referenced International Section 214 application. The response includes confidential and proprietary information that is highly competitively sensitive. Accordingly, pursuant to Section 552(b)(4) of the Freedom of Information Act (“FOIA”),¹ the Applicant requests that the response be given confidential treatment in its entirety.



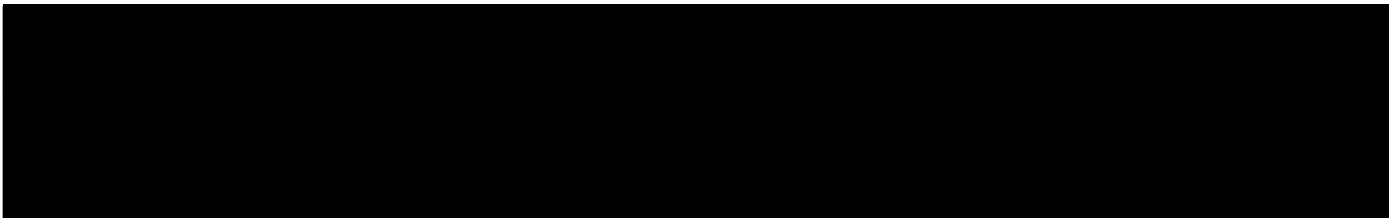
¹ 5 U.S.C. § 552(b)(4). Exemption 4 of the FOIA provides that an agency need not disclose “trade secrets and commercial or financial information obtained from a person which is privileged or confidential.”

Team Telecom
November 3, 2011
Page 2



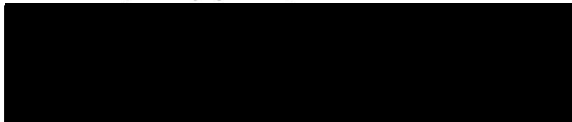
WILKINSON) BARKER) KNAUER) LLP

Team Telecom
November 3, 2011
Page 3



Please direct any questions regarding China Mobile USA's response, including this request for confidential treatment, to the undersigned.

Very truly yours,



Jennifer L. Kostyu
Counsel to China Mobile International (USA) Inc.

Enclosures

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 2

DOJ Triage Questions

Questions for FCC Applicants Reviewed by Team Telecom


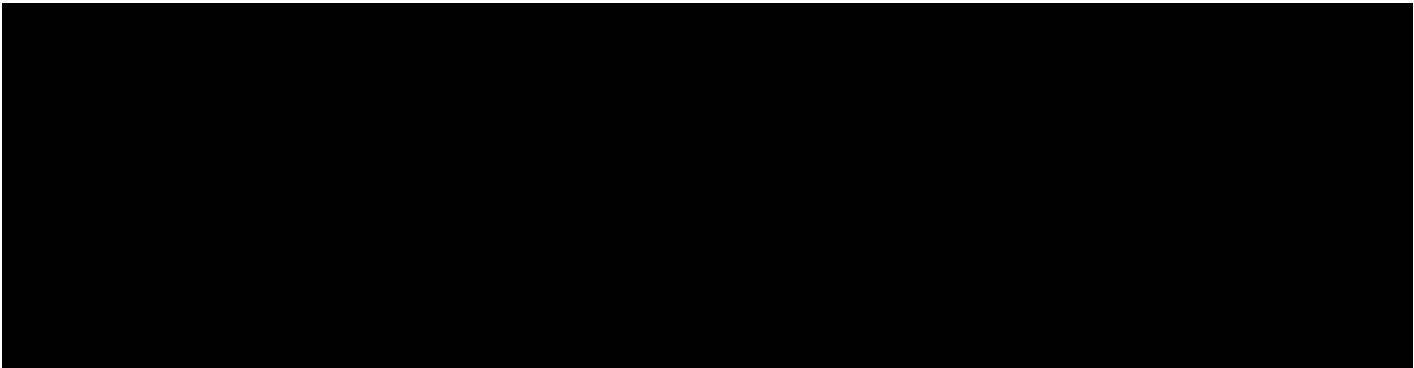
Company Name: China Mobile International (USA) Inc.
Company Address: 707 Wilshire Blvd.
Suite 5388
Los Angeles, CA 90017

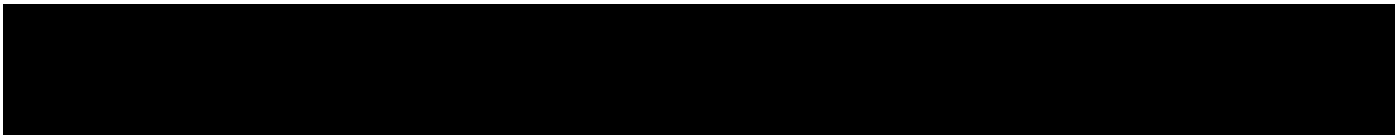
FCC Application #:
ITC-214-20110901-00289
Place of Incorporation:
Delaware

This list of questions solicits information that Executive Branch Agencies, participating in a working group informally known as “Team Telecom” (Department of Homeland Security, Department of Justice, including the Federal Bureau of Investigation, and the Department of Defense), will use to address homeland security and law enforcement concerns on the above-referenced Federal Communications Commission licensing application. Your application to the FCC indicates that you are seeking **Global or Limited Global Facilities-Based and Resale** Authority. In addition to seeking further details regarding your company and security-related practices, the following questions are particularly directed at identifying and assessing the complete scope of the equipment which you will be operating and the services which you will be offering should the FCC grant those authorities. Accordingly, in answering questions in Section III (Company Services) and the Services Portfolio Checklist and Reference Questions in Section IV, please be as complete as possible with particular attention to all switches and routing equipment and all services offered in retail markets.

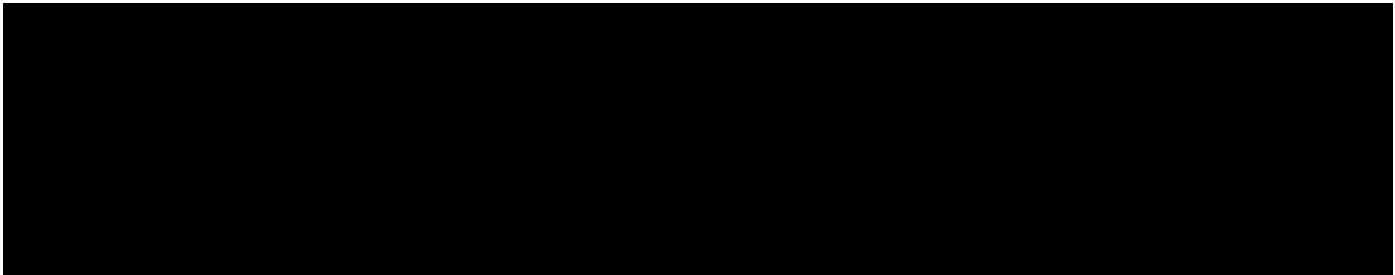
Instructions for Sections I, II & III: Please complete all Sections. When a “Yes” answer is indicated, please provide further information as appropriate. Any documents or responses to Team Telecom’s triage questions that contain trade secrets or commercial or financial information that are privileged or confidential should be identified as such.

Section I: Applicant Company Details

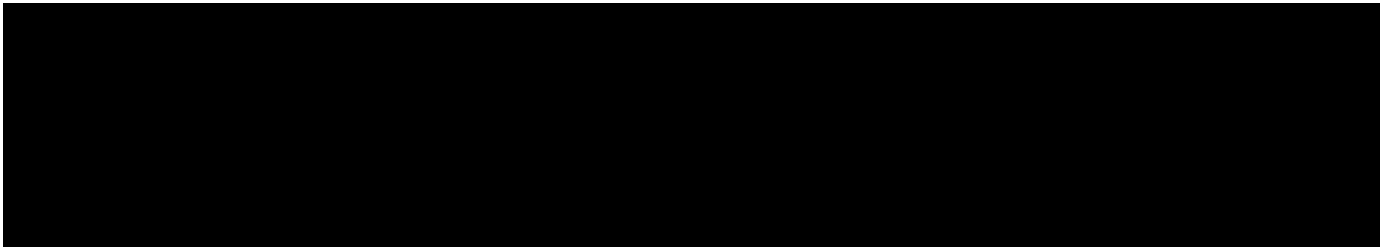
- 1) Does the Applicant have existing (or planned) relationships/partnerships with any foreign companies and/or any foreign government-controlled companies? 
If yes, indicate whether the relationship/partnership includes a management role by any foreign companies. Provide the name(s) of the individuals and foreign companies and explain the nature of the relationship, including whether the relationship currently exists and/or is intended to continue in the future.
- 

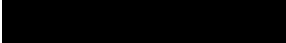


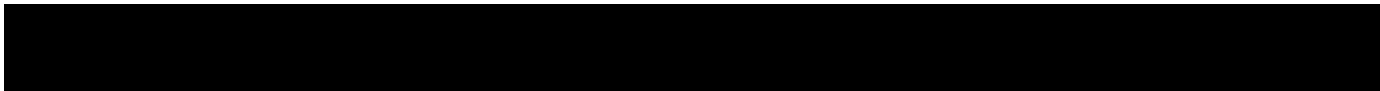
- 2) Identify the total number of current employees, and planned number of employees for the next 12 months.




- 3) Will any non-U.S. citizen, including management, have access to one or more of the following:




- a) Physical facilities and/or equipment under the Applicant's control? 
If yes, provide identity of person(s)¹ and explain the type of access that will be provided.

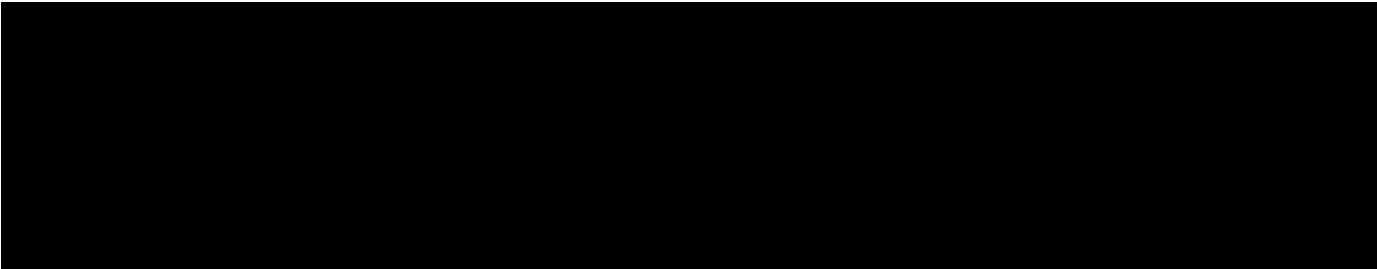



- b) Customer records, including Customer Proprietary Network Information (CPNI), billing and Call Detail Records (CDRs)? 
If yes, provide identity of person(s) and explain the type of access and records that will be provided.

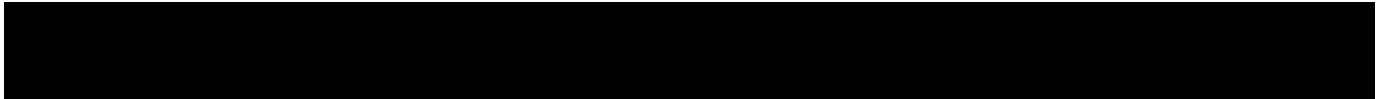


- c) Network control, monitoring, and/or auditing features? 
If yes, explain the type of access that will be provided, and how access will be logged and archived.

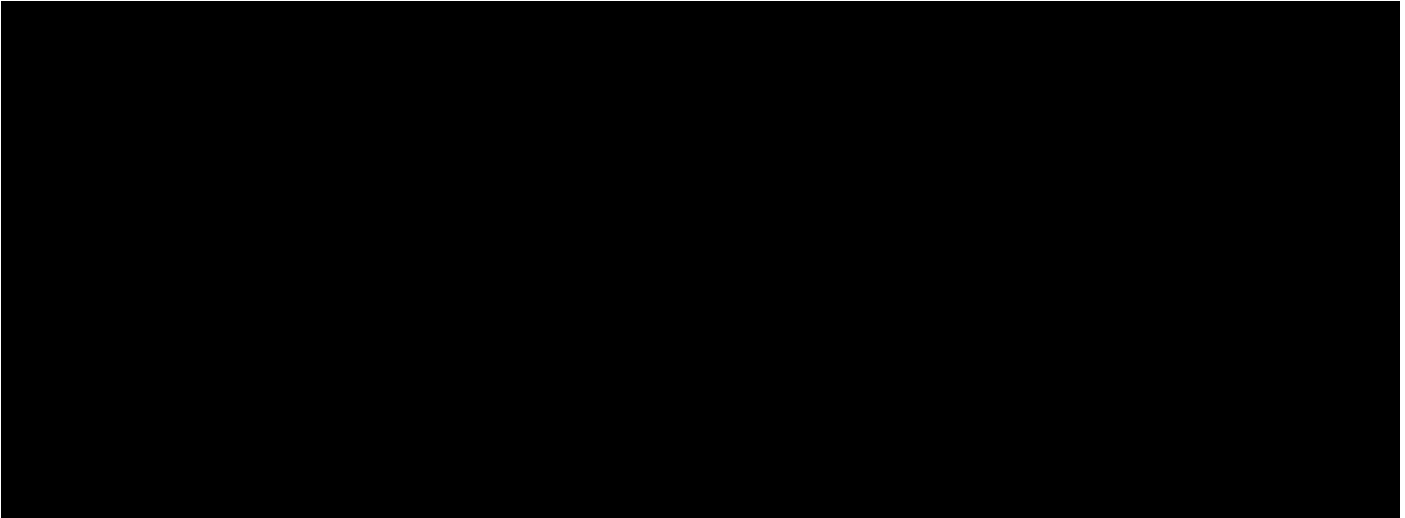
¹ For each such individual, provide name, country of citizenship, date and place of birth, U.S. alien number (if applicable), passport identifying information (including number and country), all residence addresses, all business addresses and all phone numbers.



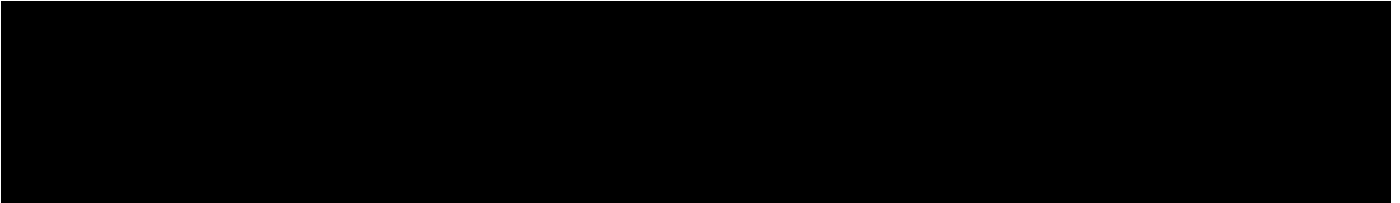
- d) Electronic interfaces that allow control and/or monitoring of the infrastructure under the Applicant's control including, but not limited to, access to actual communications content and data? 
If yes, provide identity of person(s) and explain the type of access and control that will be provided.



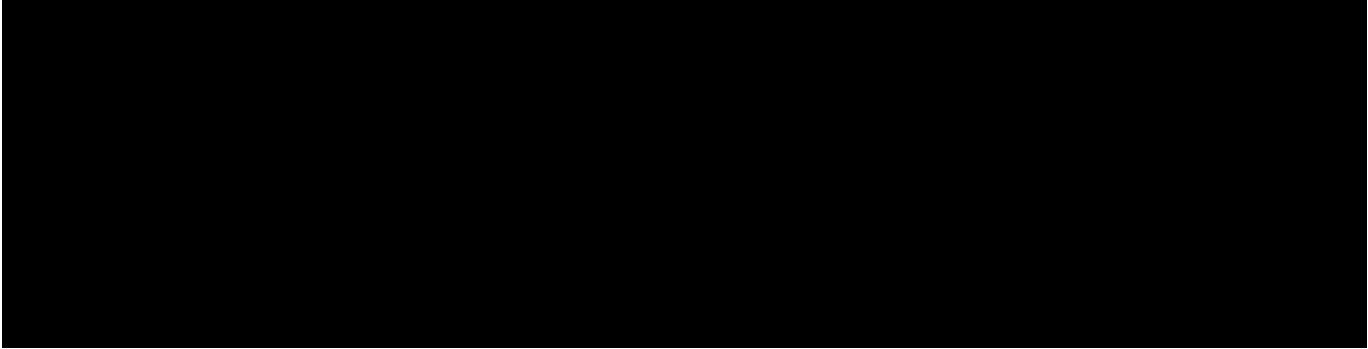
- 4) What access control/security policies are in place for your production network?



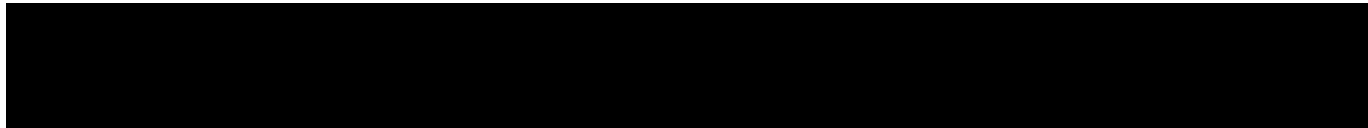
- 5) What encryption products/technologies have been installed on this production network?



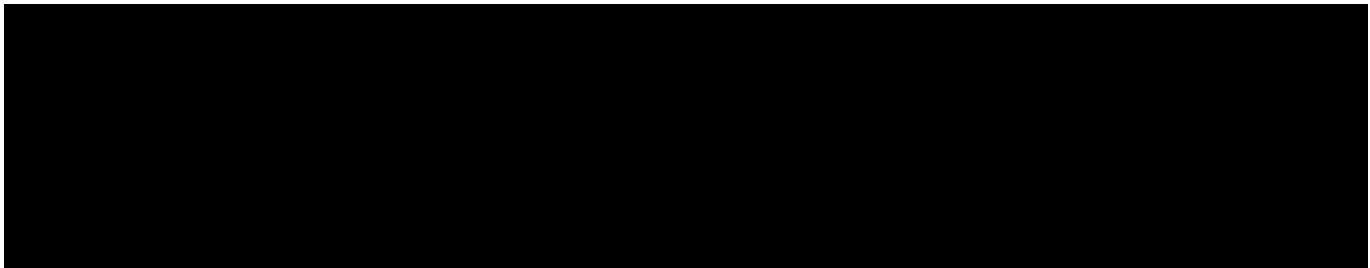
- 6) Does the Applicant have any screening and/or vetting procedures which will be applied to U.S. or non-U.S persons who have access, remote or otherwise, to the Applicant's communications network facilities, equipment, or data? [REDACTED]
If yes, explain all such procedures.



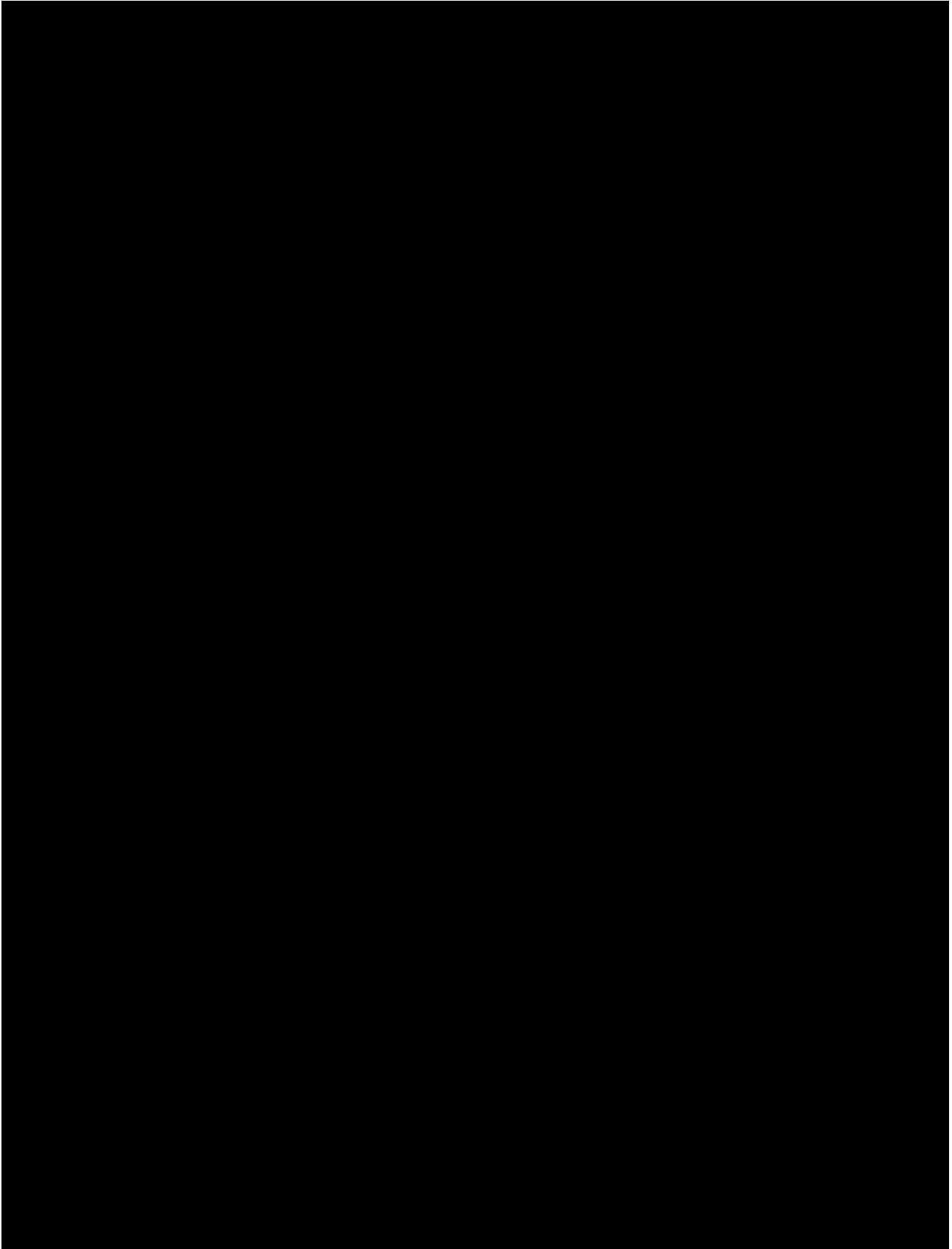
- 7) Does the company currently operate or plan to operate a website? [REDACTED]
If yes, provide all URL addresses for any current or known future company sites and describe whether the information therein is up to date.

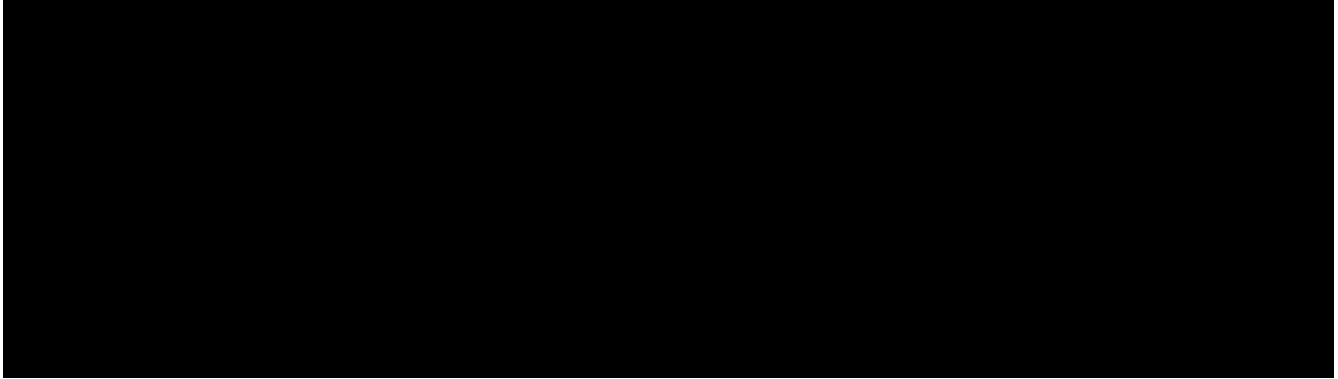


- 8) Provide all addresses of the present and anticipated physical locations for all of the Applicant's network equipment and infrastructure, whether owned or leased.



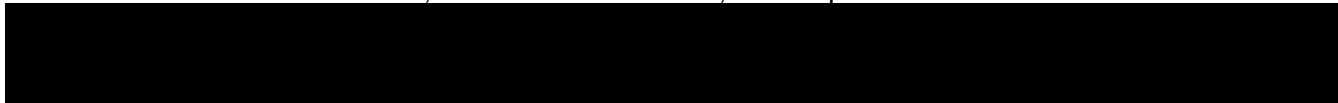
- 9) Identify each individual or entity, whether direct or indirect, holding or controlling greater than a 5% equity stake in the Applicant company (whether voting or non-voting), highlighting any foreign government entities. Please be sure to include the ultimate parent owner of the Applicant and any other companies/individuals owning more than a 5% equity stake in the chain of ownership.



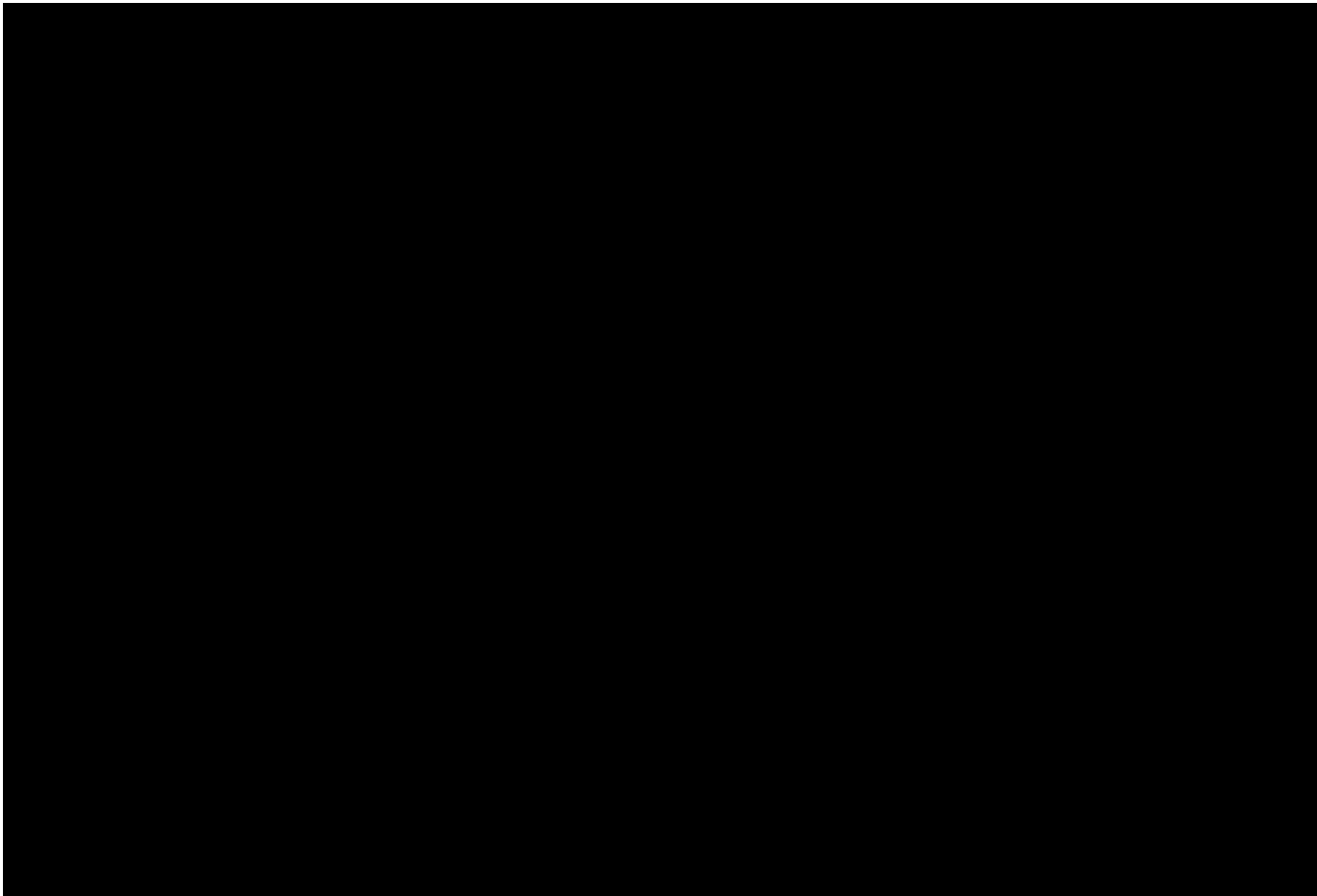


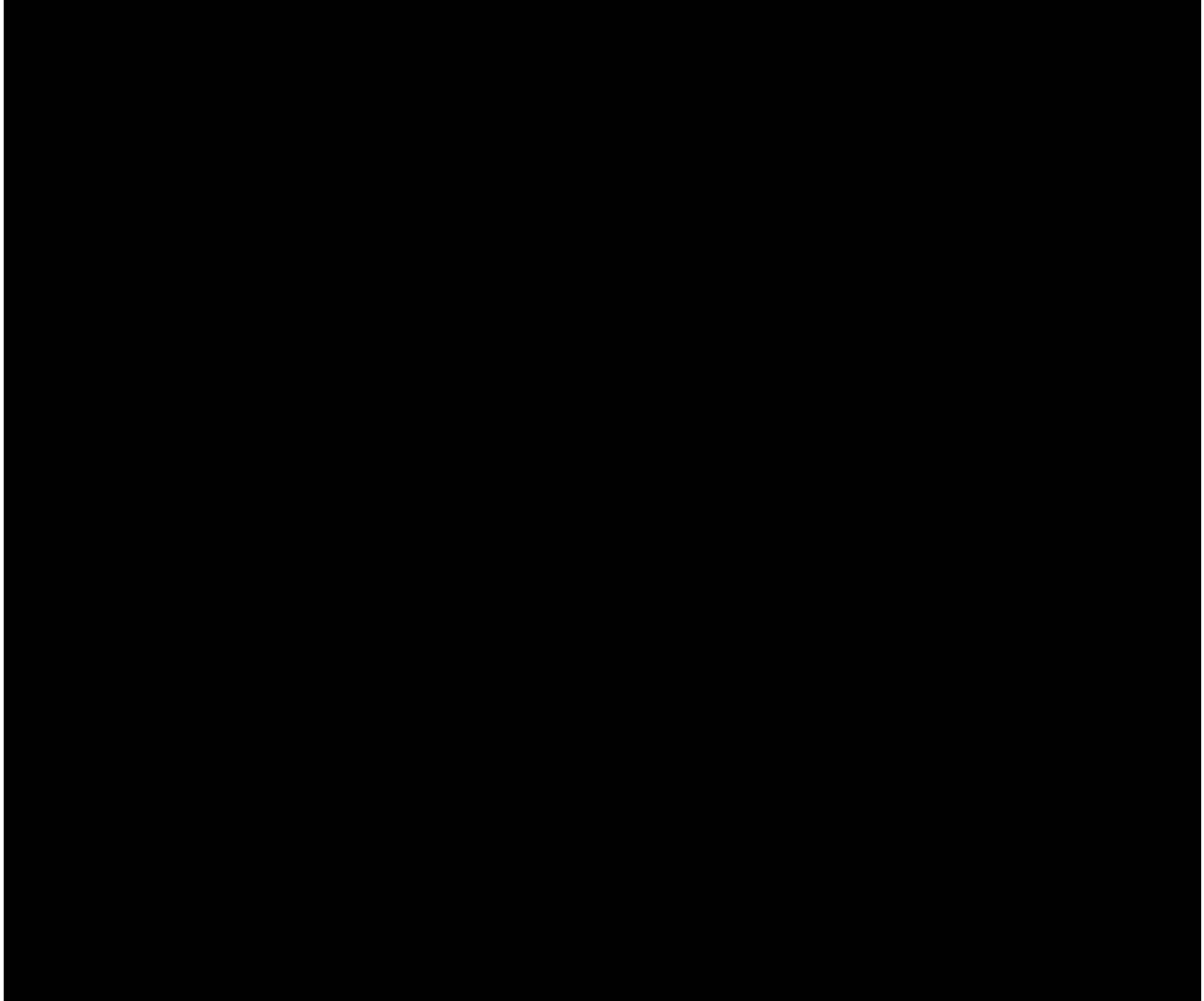
b) For each such individual or entity, provide all identifying information, as follows:

i) For individuals, provide name, citizenship, date and place of birth, U.S. alien number (if applicable), passport identifying information (including number and country), all residence addresses, all business addresses, and all phone numbers.





ii) For entities, provide country of incorporation/main place of business, general business type (e.g. holding company, investment firm, etc.), all business addresses, and related phone numbers.





10) Has the Applicant company, any company officers/directors or any individual/company with 10% or greater ownership interest in the Applicant company, ever been investigated, arraigned, arrested, indicted or convicted of any of the following:

- i. Espionage-related acts, or criminal acts including violations of the International Trade in Arms Regulations (ITAR), the Export Administration Regulations (EAR), or other US law?

- ii. Deceptive sales practices, violations of the Consumer Fraud Act and regulations, and/or other fraud or abuse practices whether pursuant to local, state or federal law?

- c) Violations of local, state or federal law in connection with the provision of telecommunications services, equipment and/or products and/or any other practices

regulated by the Telecommunications Act of 1996 and/or by state public utility commissions? [REDACTED]

If yes to any of the above, please describe in detail, including name(s) of company officials and/or company involved, date(s), and current status or final disposition of matter, including any terms of settlement.

Section II: Applicant Company Operations

1) Has the company been operational over the course of the current and previous year?

[REDACTED] If yes, answer the following:

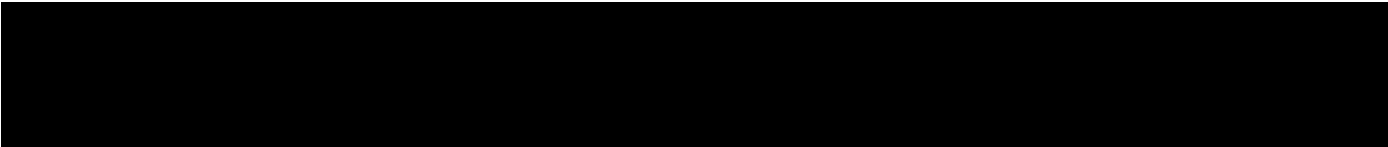
- a) Provide separately for each year the Cost of Goods Sold (COGS).
- b) What was the total amount of COGS allocated for telecommunications equipment and service types?
- c) Describe, for all services provided to each category of customer (e.g. enterprise, residential, carrier, etc.):
 - i. Total number of subscribers;
 - ii. Total annual gross revenue for preceding fiscal year;
 - iii. Percentage of total gross revenue per category of customer for preceding fiscal year.

2) List all expected and actual Federal, State, and local government customers including any classified contracts, and include a description of all services to be provided, or services that are currently being provided, to such customers.

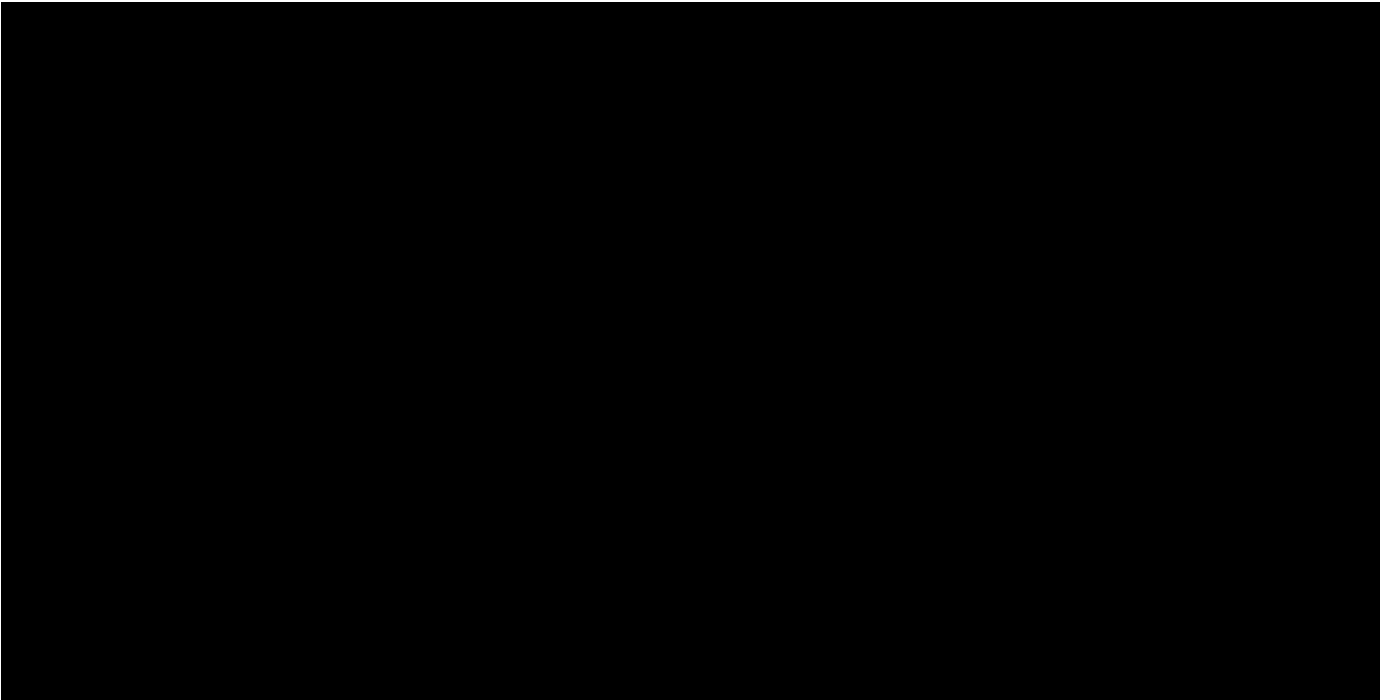
[REDACTED]

3) For each member of the Applicant's senior management team, list the names (where applicable) of the CEO (Chief Executive Officer), President, CFO (Chief Financial Officer), CIO (Chief Information Officer), CTO (Chief Technical Officer), COO (Chief Operating Officer), Senior VPs, and any other positions involved in exercising day-to-day management responsibilities:

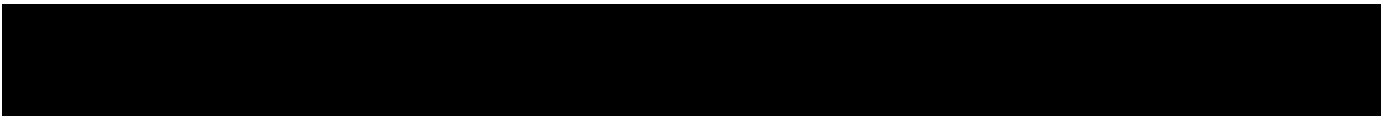
a) Explain the nature and extent of each senior manager's involvement in the company; and



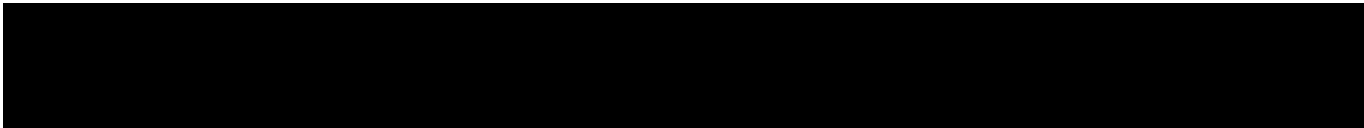
- b) Provide each senior manager's name, citizenship, date and place of birth, U.S. alien number (if applicable), passport identifying information (including number and country), all residence addresses, all business addresses and all phone numbers.




- 4) Identify a senior officer or employee (U.S. citizen or legal alien residing in the U.S. with an active security clearance or able to obtain one) who will be the Applicant's authorized law enforcement point of contact responsible for accepting and overseeing compliance with subpoenas/court orders/search warrants including responding to official requests and/or compulsory processes from U.S. law enforcement or other U.S. government agencies.




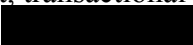
- a) For this individual, explain the relationship to the Applicant and provide name, citizenship, date and place of birth, U.S. alien number (if applicable), all passport identifying information (including number and country), all residence addresses, all business addresses and all phone numbers.



b) Confirm that the Applicant will report to the appropriate law enforcement agencies, immediately upon discovery:

i) Any act of compromise of a lawful interception of communications or access to call-identifying information to unauthorized persons or entities? 

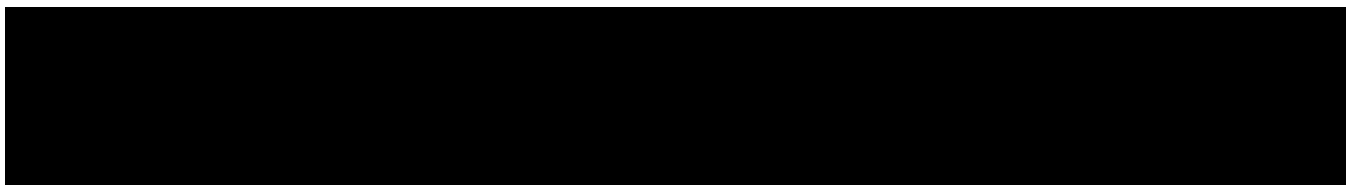
ii) Any act of unlawful electronic surveillance that occurred on its premises or via electronic systems under its control? 

5) Will the Applicant store and/or maintain any U.S. communications content, transactional data, call-associated data, billing records or other subscriber information? 
If yes, please answer the following:

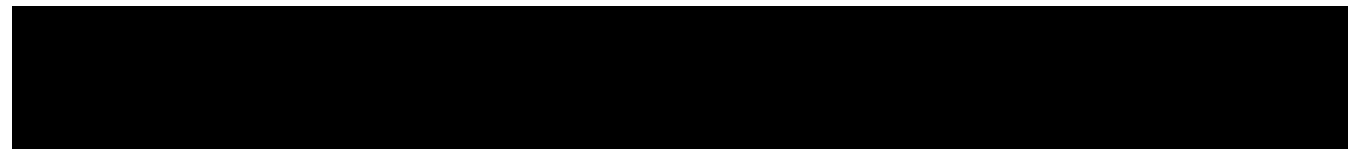
a) Describe what types of records will be stored.



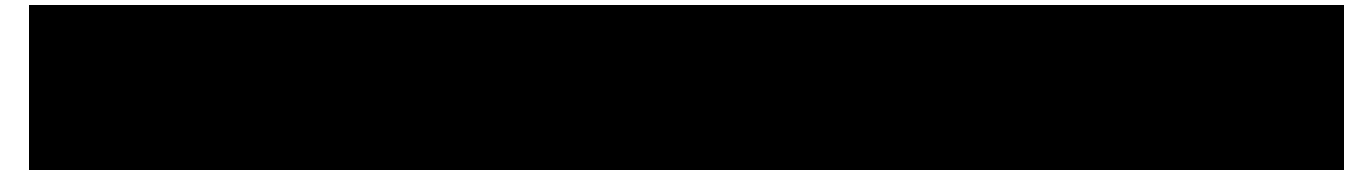
b) Provide all addresses of locations where such records will be stored and/or remotely accessed/managed via electronic systems.

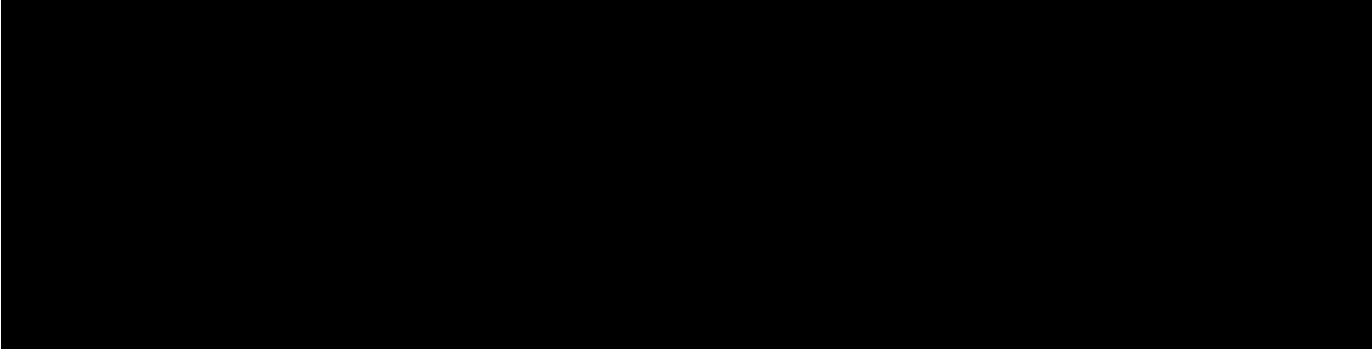



c) If any storage location differs from the Applicant's address, explain the general purpose of the location and its function within the Applicant's business.




d) Describe all physical/electronic security measures utilized for all locations/systems to protect the confidentiality of records.

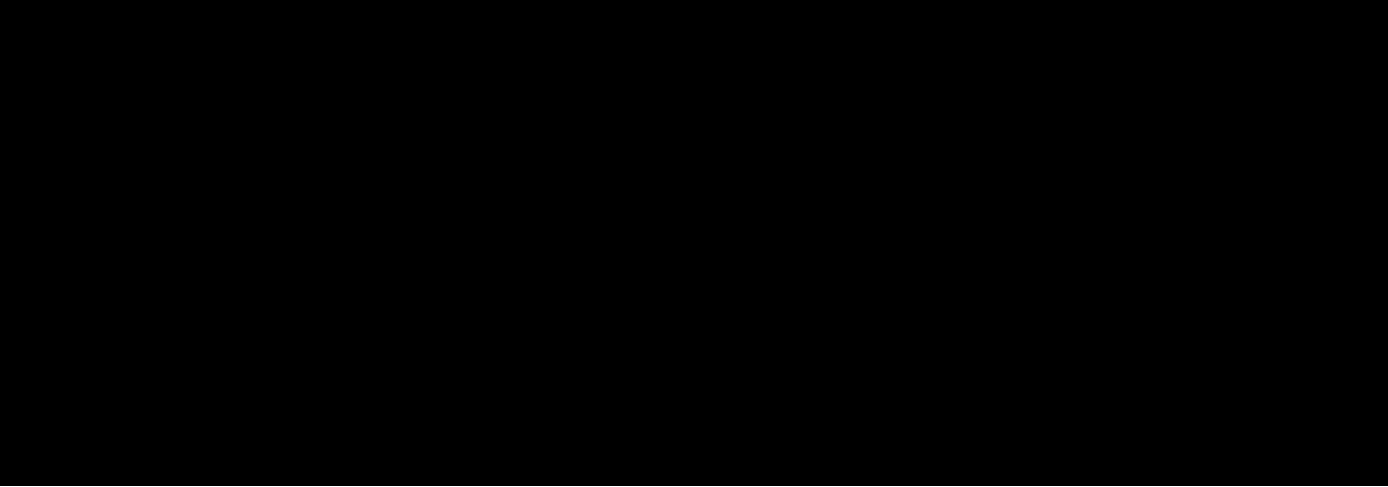





e) Confirm that the Applicant will inform the National Security Division (NSD) of the U.S. Department of Justice if, in the future, any record storage/access location is transferred and/or newly established outside of the U.S. 

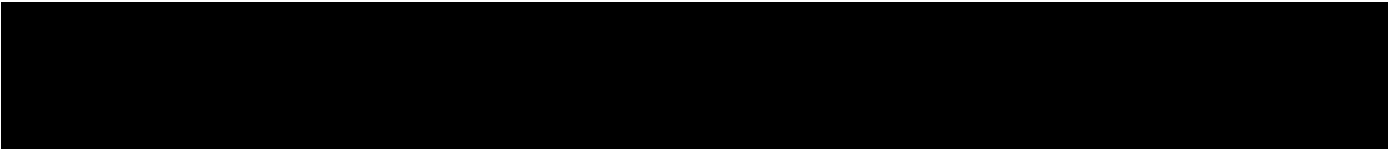
f) Can the Applicant agree to make any and all records not stored in the U.S. electronically available in the U.S. within five business days of law enforcement serving legal process through the Applicant's U.S. based point of contact (identified in question 4 above)? 

6) Describe the Applicant's lawful intercept solution(s). Include all lawful intercept capabilities of the Applicant company to include whether the Applicant uses (or intends to use) a Trusted Third Party (TTP) provider. If so, please provide the name of that TPP and whether the Applicant has a signed agreement with that TPP. If the Applicant will use its own equipment, please specify the equipment and describe the functions supported.

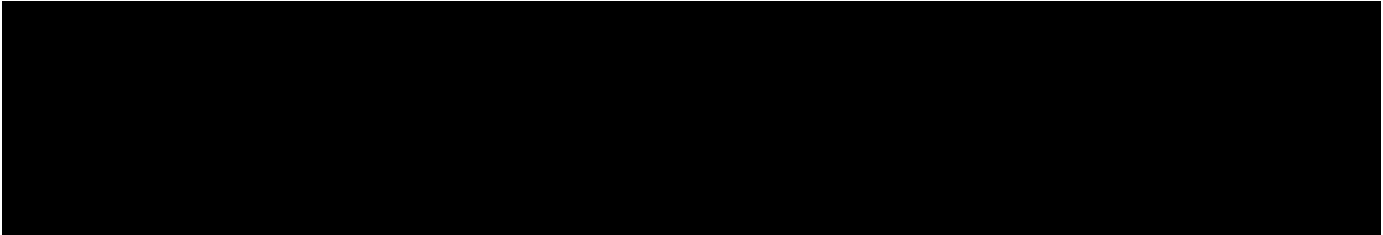


7) Describe the customer base of the Applicant company (business, residential, carrier, enterprise, etc.).



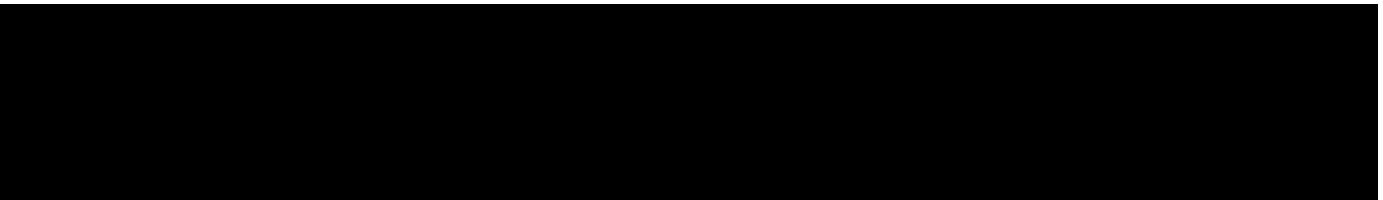


- 8) What, if any, outside capabilities via remote access will exist within the Applicant company to control operations over the network (e.g., audit mechanisms, record access monitoring)?

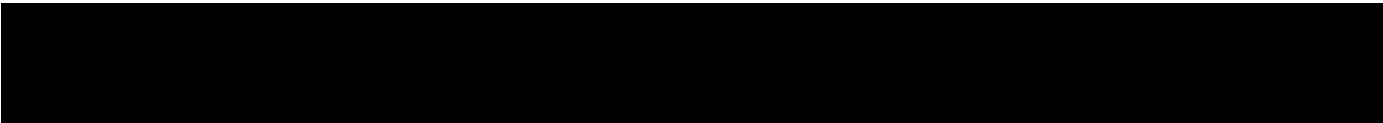



Section III: Applicant Company Services

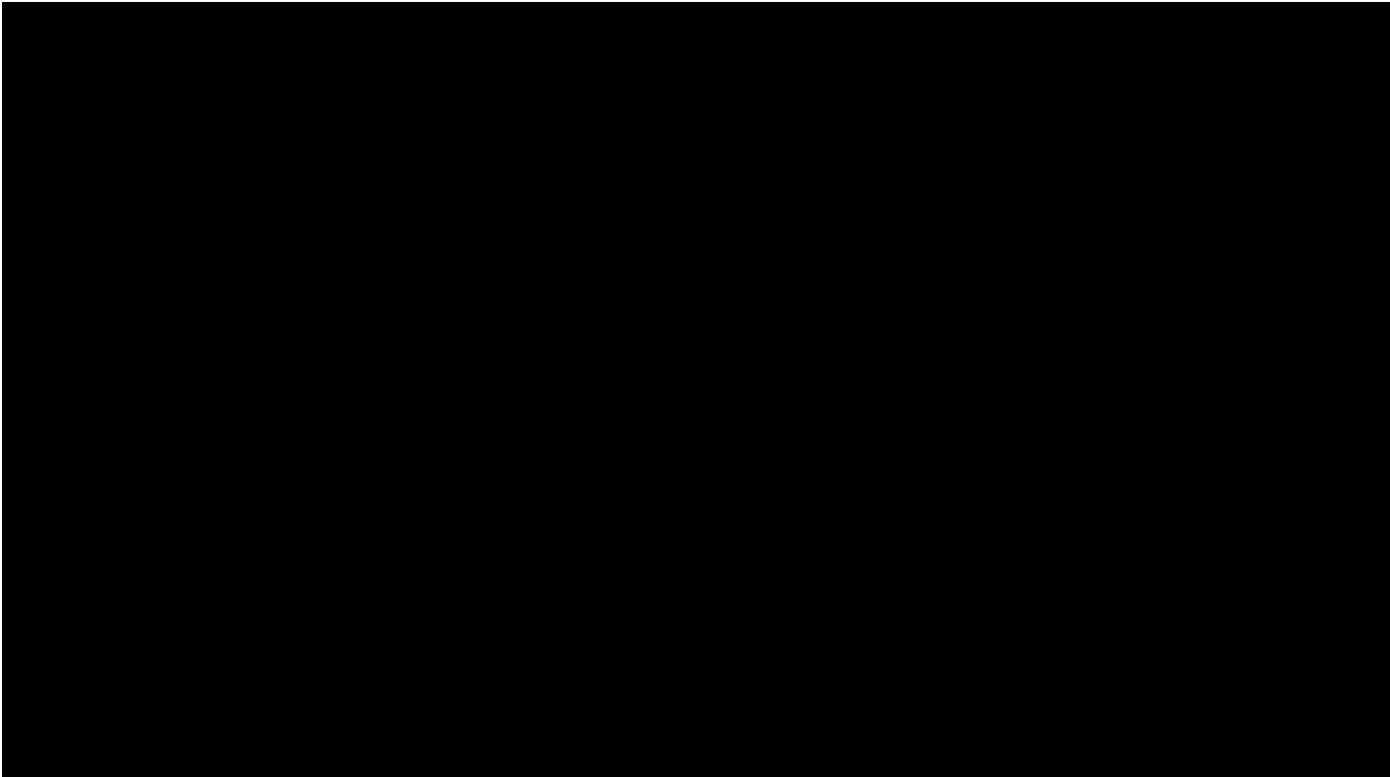
- 1) Provide a general summary of the nature of the Applicant's current and planned services and operations, to include an explanation of the Applicant's intended overall business model and its relationship with any sister and/or partner companies.



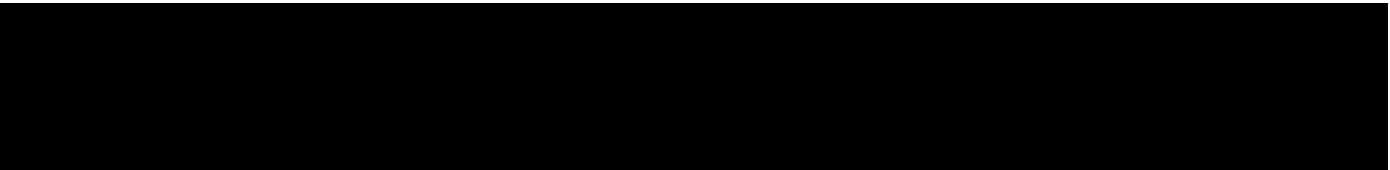
- 2) Describe the carrier transport facilities (T1, DS3, Optical Carrier) that will enable customer data flow into and out of owned and/or leased equipment.




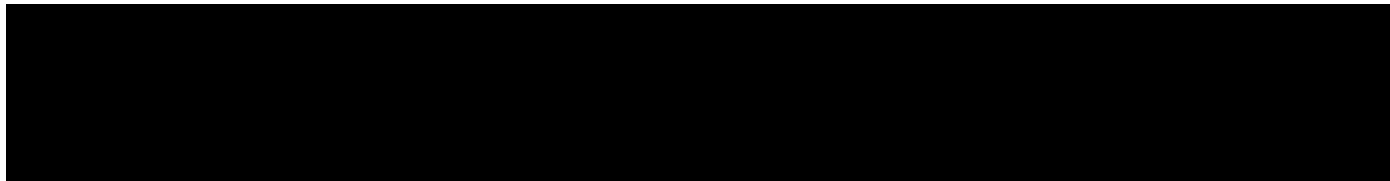
- 3) Will the Applicant be operating any physical telecommunications switching platforms (TDM and/or VoIP switches)? 
If yes, provide a network architecture diagram that shows all switches and connection points.




- 4) Provide a description of any other intended network equipment and/or proposed infrastructure (e.g., routers, media gateways, multiplexing/cross-connect facilities, signaling devices, other equipment).




- 5) Does the Applicant have a network topology map that shows it's Points of Presence (POPs) and/or a geographic footprint? 
If yes, attach to Questionnaire. If not, describe the network topology as clearly as possible.

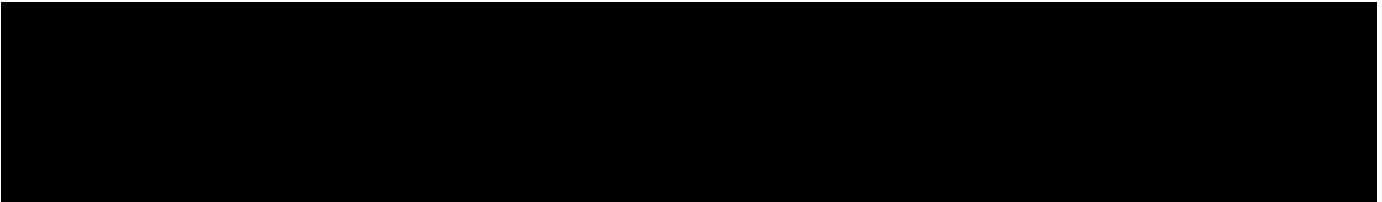



- 6) Will the Applicant company use interconnecting carriers and/or peering relationships? 
If yes, provide details and list the carriers.

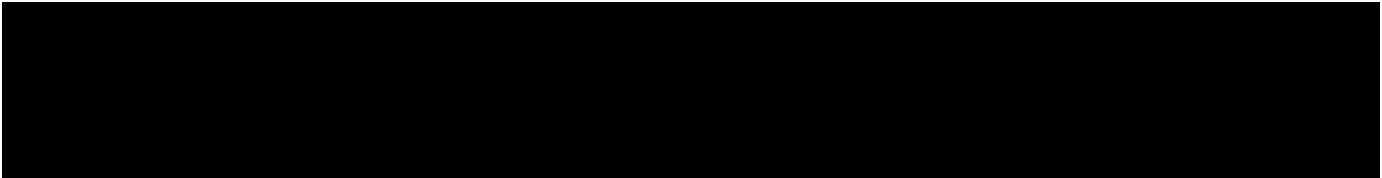




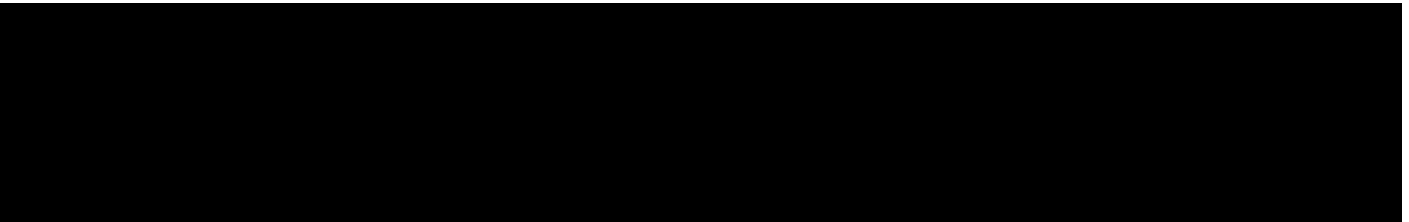
- 7) Will the Applicant rely on underlying carrier(s) to furnish services to its customers and/or resell any services? 
If yes, provide details and list whose services will be resold.



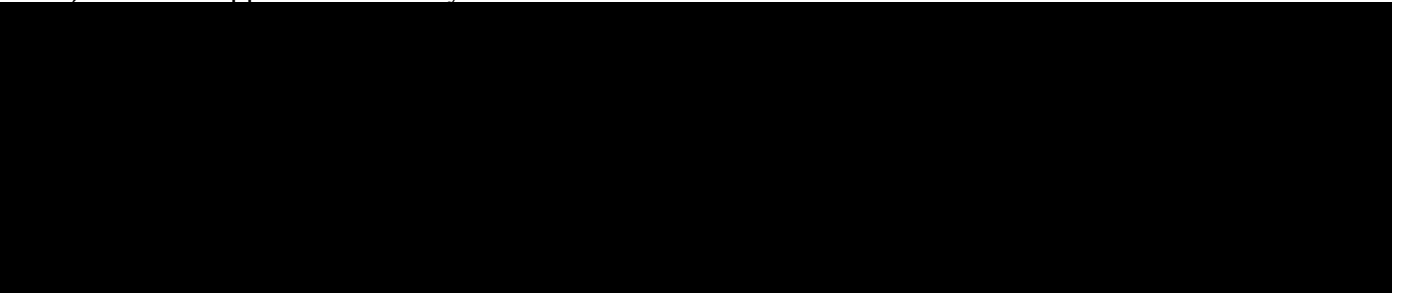
- 8) Is the Applicant or its affiliates able to control operations at any POP and/or Network Operations Center (NOC) from any overseas locations? 
If yes, what is the nature of the foreign-based control?

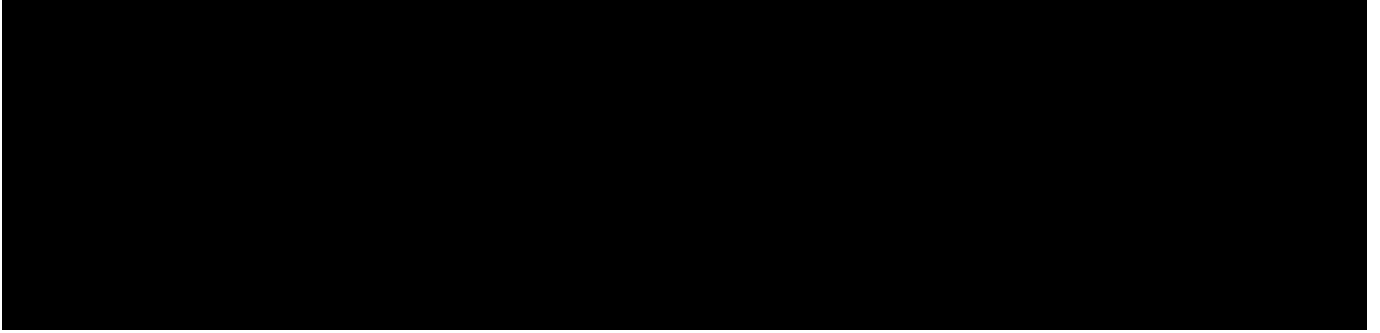


- 9) What services will be delivered to customers, and how will the services be delivered?



- 10) Does the Applicant serve any sectors of U.S. critical infrastructure?



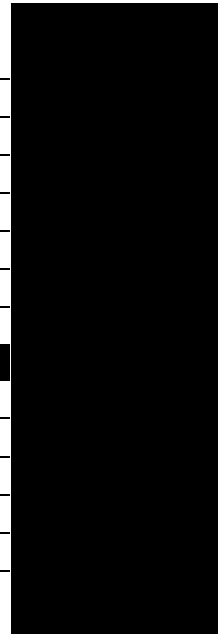


Section IV: Applicant Company Services Portfolio Checklist

*Instructions: Please check all applicable boxes that reflect the types of telecommunication services the Applicant intends to provide **in the U.S. only**. **Do not select any services that will be provided outside the U.S.** For each checked box, please provide a **separate** and full explanation at the end of this questionnaire, as well as answer the Reference Questions below the table as they pertain to the services you have indicated in the checklist.*

Proposed Applicant Services	
VOICE SERVICES	
VoIP (Voice over Internet Protocol)	
POTS (Plain Old Telephone Service)	
TDM (Time Division Multiplexing)	
Voicemail	
PBX (Private Branch Exchange)	
Centrex (Hosted/Managed PBX)	
Callback Service	
Calling Card	
Dial Tone Service	
Issue DID (Direct Inward Dial) Local Telephone Numbers	
Local Exchange Service	
Local Toll Service	
Domestic/International Long Distance (Interexchange Service)	
Tollfree Service	
IVR (Interactive Voice Response)	
Conference Calling	
Operator Service	
Directory Assistance	
Dial Around Service (1010XXX Casual Calling)	
Switched Access	
Special Access (Dedicated Line)	
ACD (Automatic Call Distribution)	
Other	
INTERNET AND DATA SERVICES	
ISP (Internet Service Provider)	
Data/Private Line	
VPN (Virtual Private Network)	
Web Hosting	
LAN (Local Area Network)	
WAN (Wide Area Network)	
ISDN (Integrated Services Digital Network) BRI (Basic Rate Interface)	
ISDN PRI (Primary Rate Interface)	
DSL (Digital Subscriber Line)	
Frame Relay	

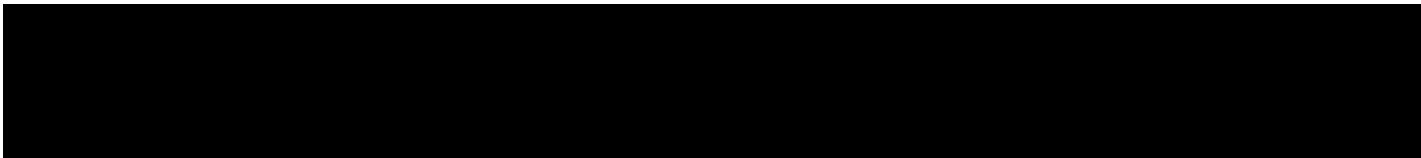
Email	
International Voice/Data Service	
Wireless/Mobile Voice/Data Services	
Satellite Services	
RF (Radio Frequency), Microwave	
Video	
Other	
CARRIER / ENTERPRISE WHOLESALE SERVICES	
Routing, Signaling Services	
Transport Facilities	
Leased Lines	
Collocation Services	
Other	



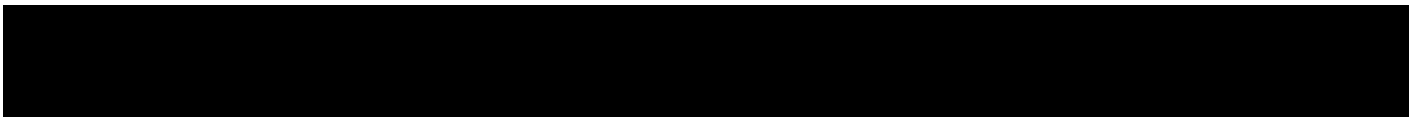
Reference Questions:

Instructions: Answer each question below as it relates to the services indicated in the above table.

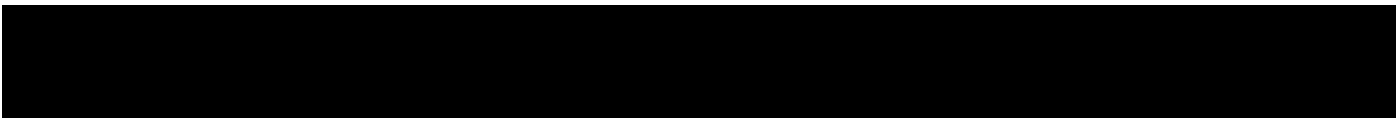
- 1) In what manner will the service(s) be delivered to your customers?
(Please describe typical customer transactions. For example: How do you acquire customers? How do customers contract services? What are your terms of sale? What are the products and services you provide? How do you deliver them?)



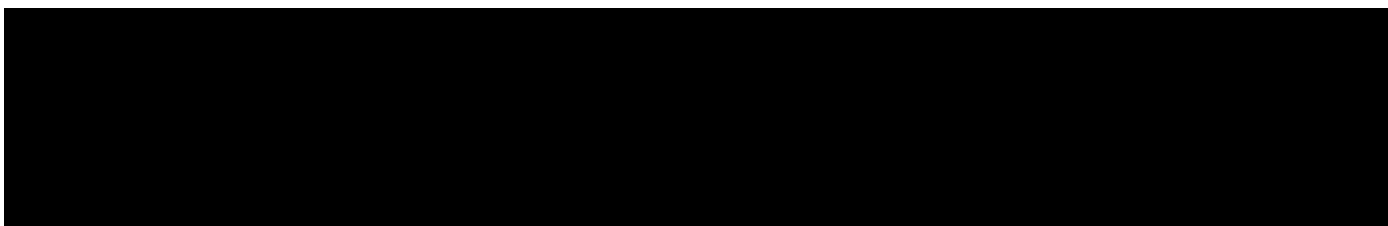
- 2) What kind of network infrastructure will be utilized to deliver the service(s)?

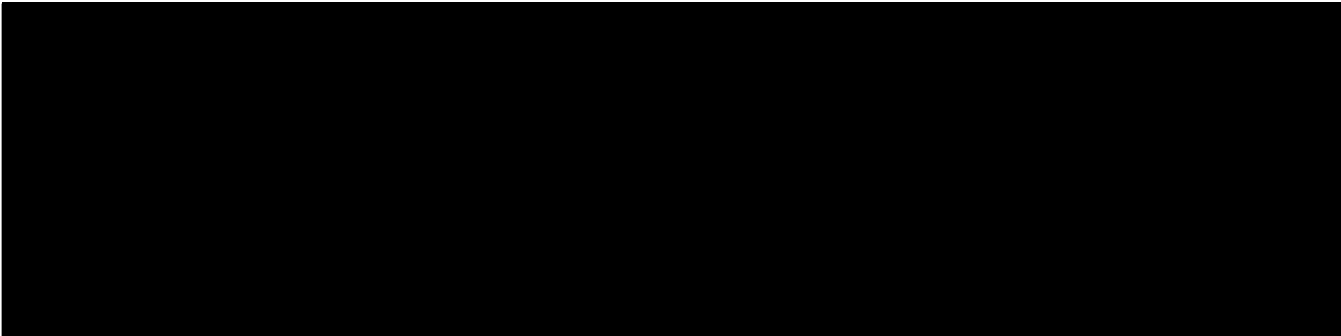


- 3) What equipment will be utilized to provide the service(s)?



- 4) Will the service(s) be facilities based, resold or both? Please describe.





Making materially false, fictitious, or fraudulent statements or representations may render the Applicant subject to fines and/or imprisonment under 18 U.S.C. § 1001.

I declare that the foregoing is true and correct to the best of my knowledge.

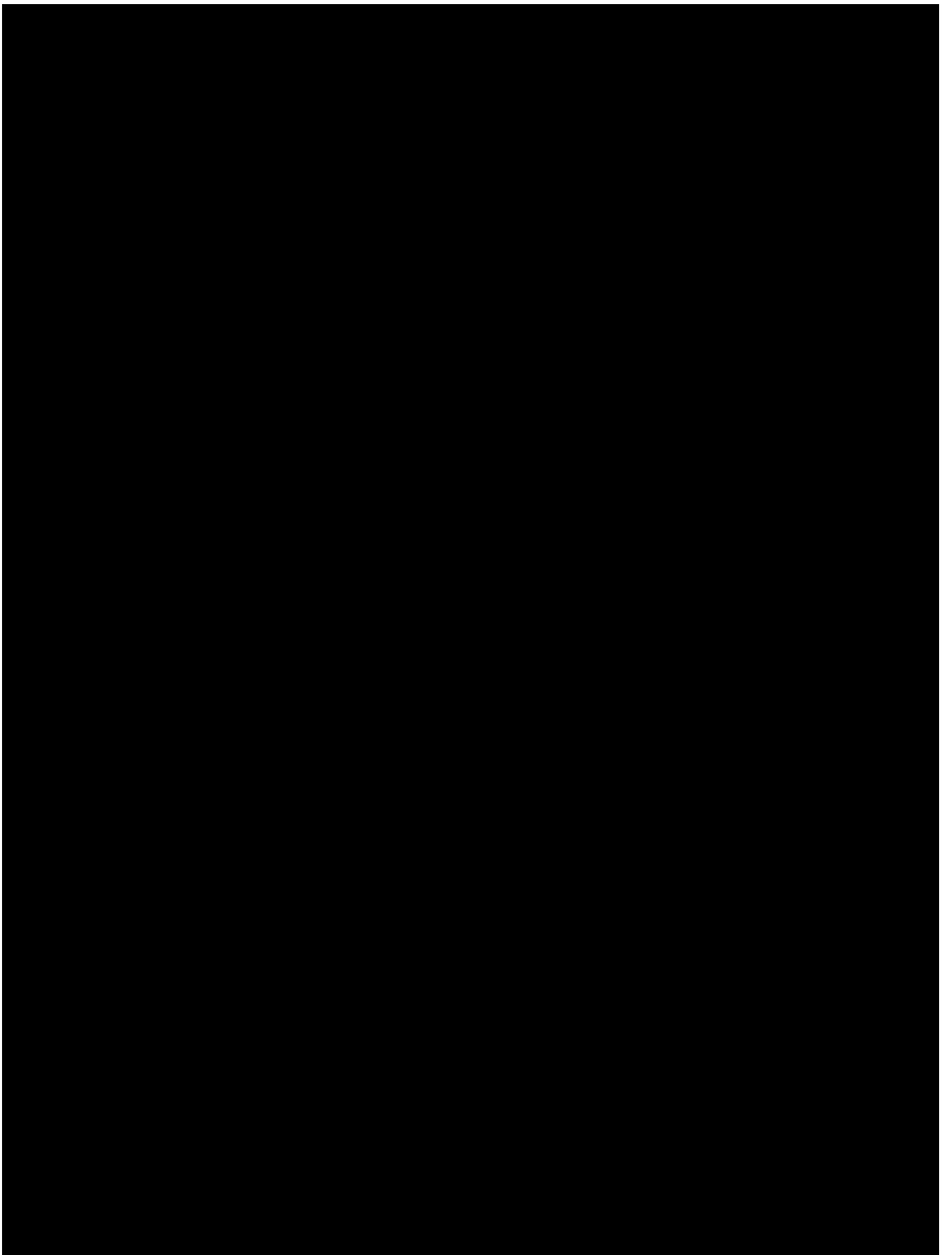
Executed this 3rd day of November, year of 2011.

X



(Applicant Signature) Director, Zhenhui LIN

Exhibit A



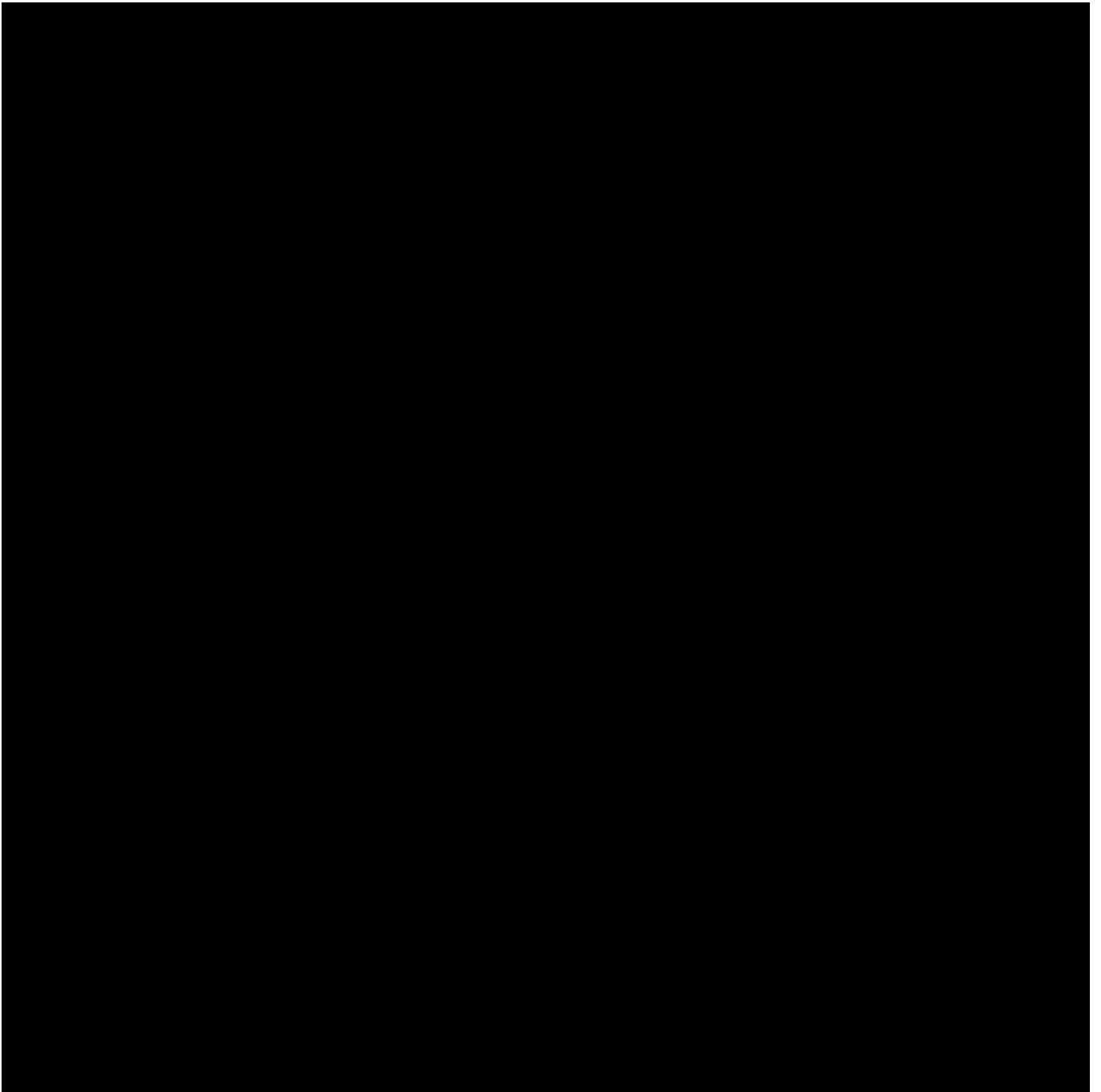


Exhibit B

Exhibit C

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 3

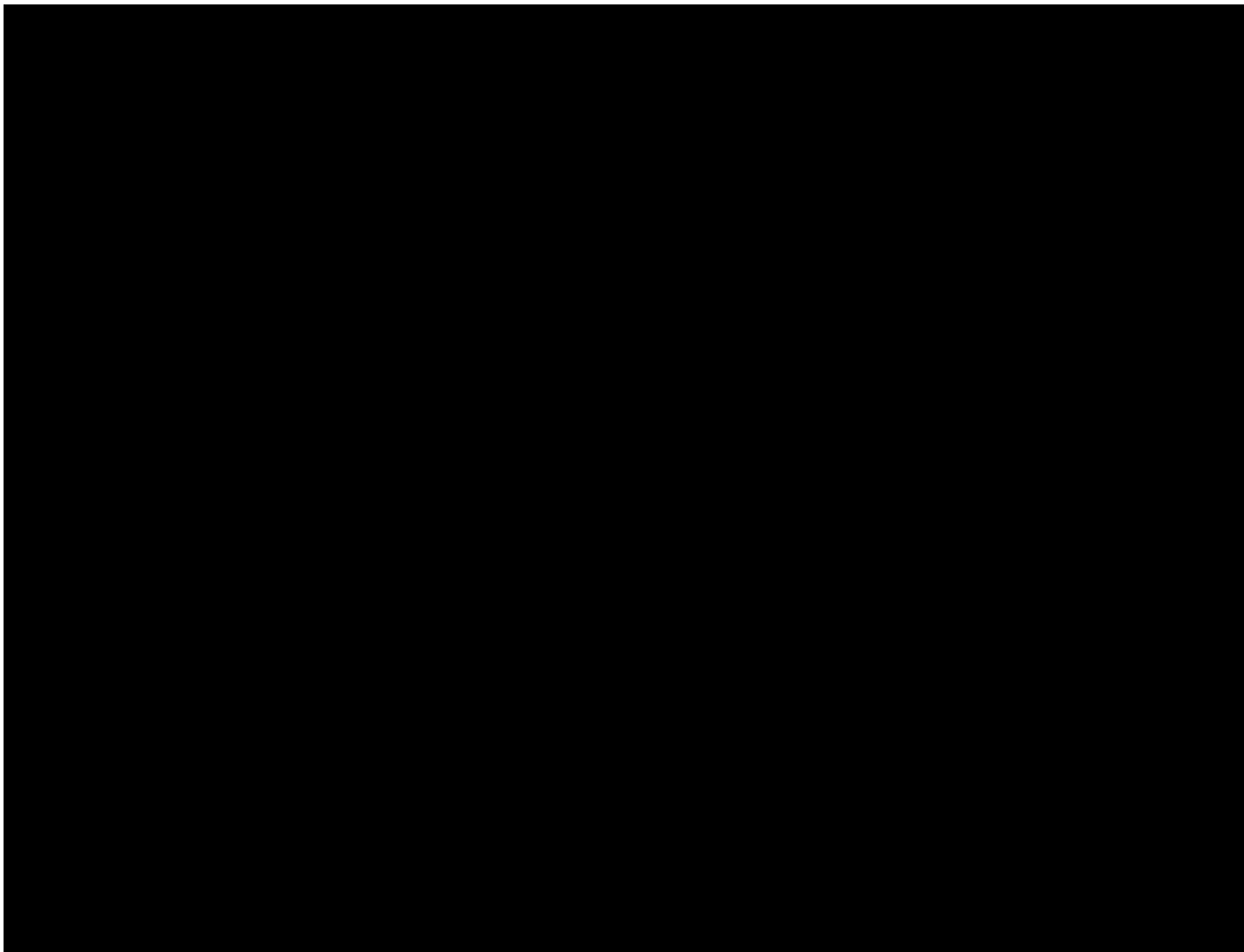
**DOJ Follow-up Triage Questions
Questions for FCC Applicants Reviewed by Team Telecom**

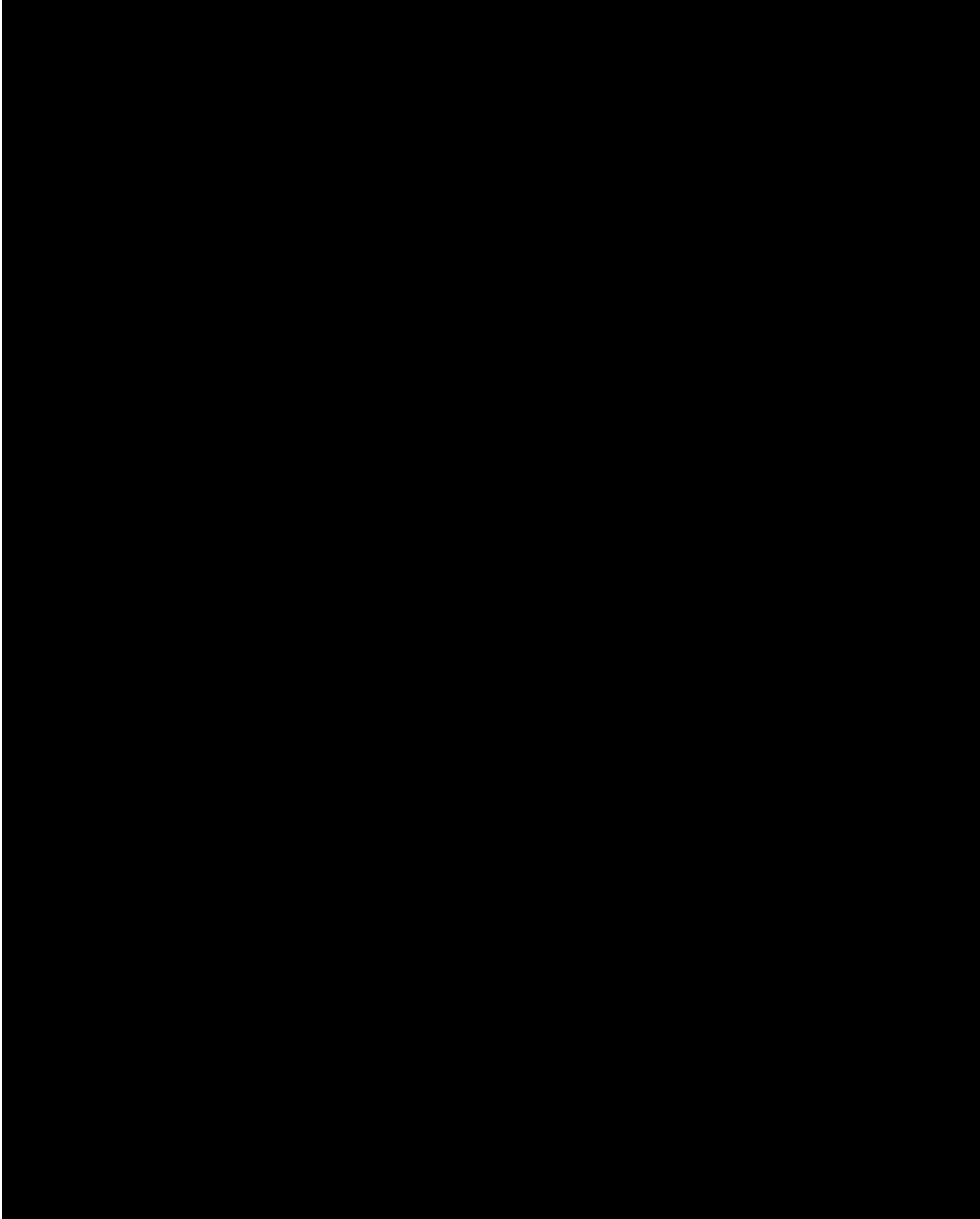
Company Name: China Mobile International (USA) Inc.

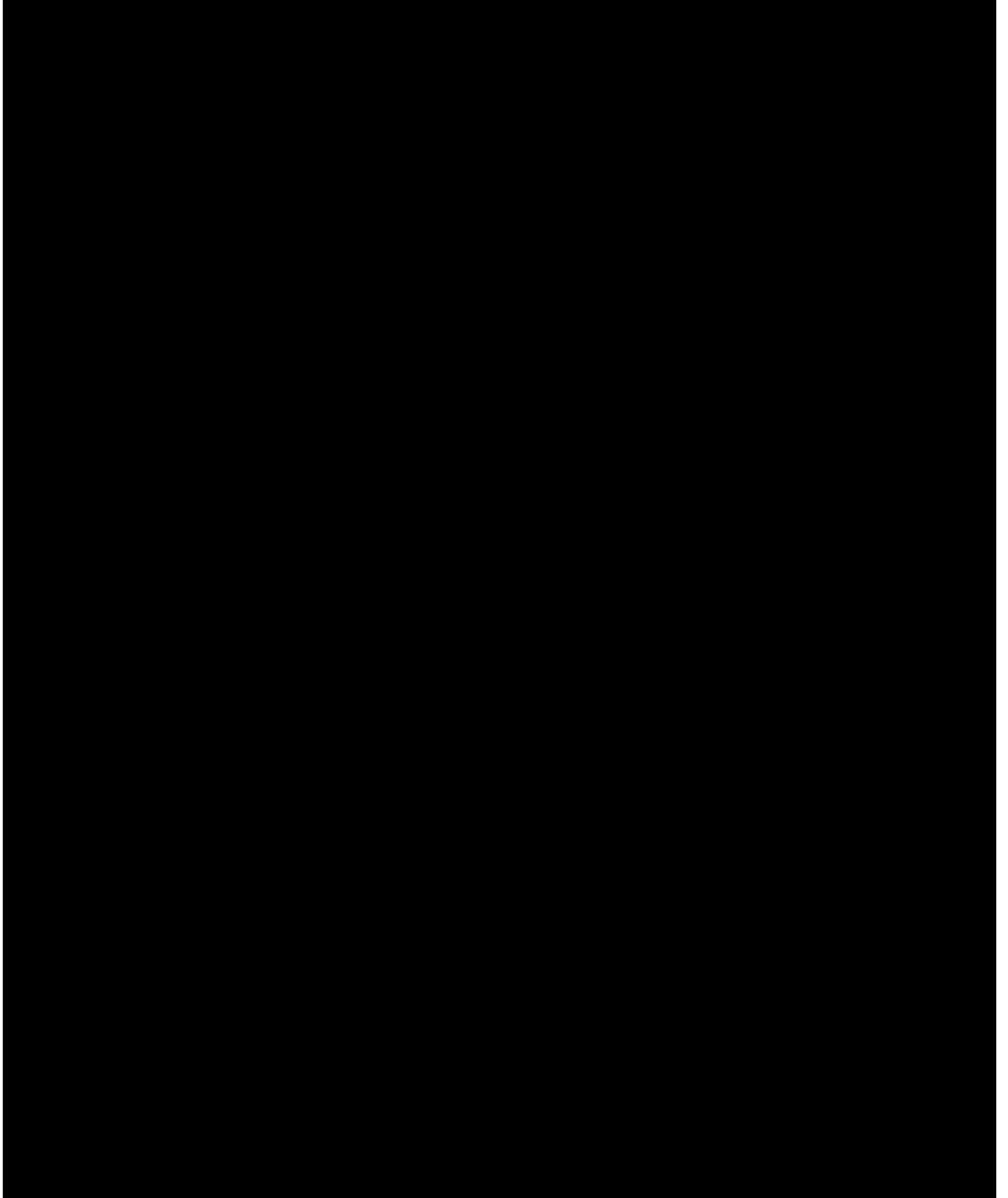
FCC Application #:
ITC-214-20110901-00289

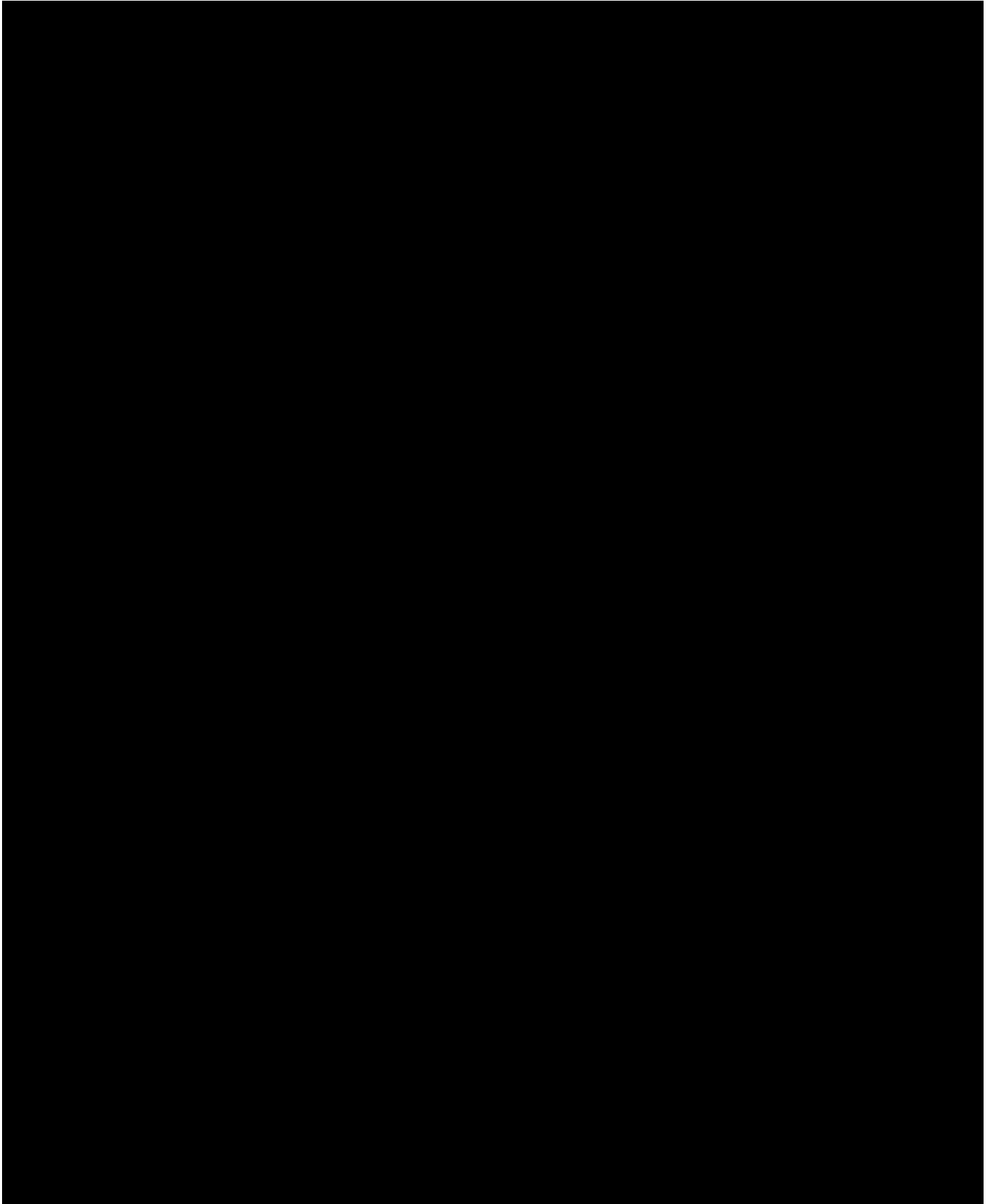
This list of follow-up questions solicits additional information that Team Telecom will use to address homeland security and law enforcement concerns on the above-referenced Federal Communications Commission licensing application. Please respond to the following questions in order to clarify China Mobile's answers to the triage questions.

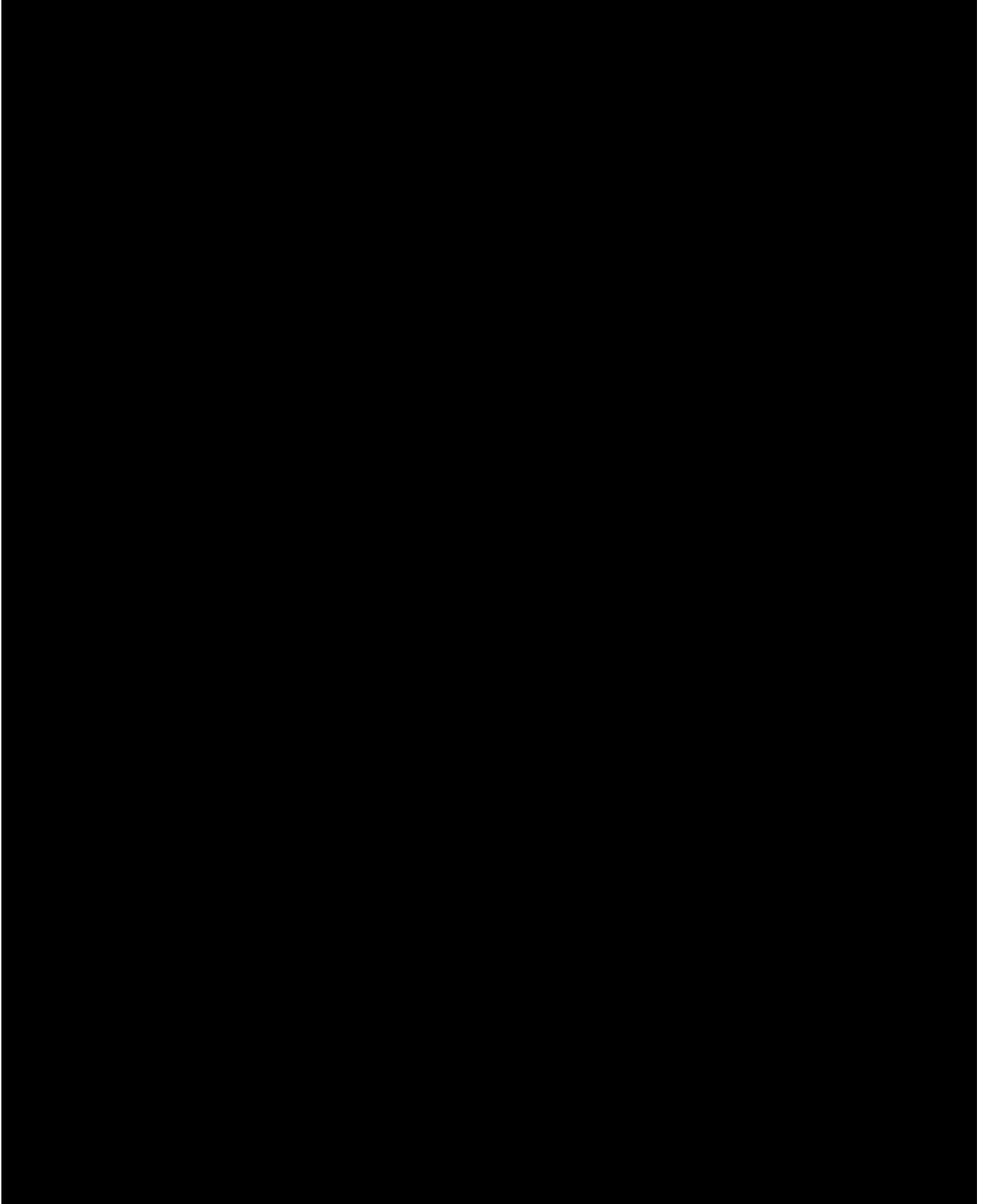
China Mobile International (USA) Inc. ("China Mobile") hereby responds to Team Telecom's following questions of February 28, 2012, in order to clarify China Mobile's earlier answers to the triage questions. China Mobile's responses are provided in blue text below following each supplemental triage question.

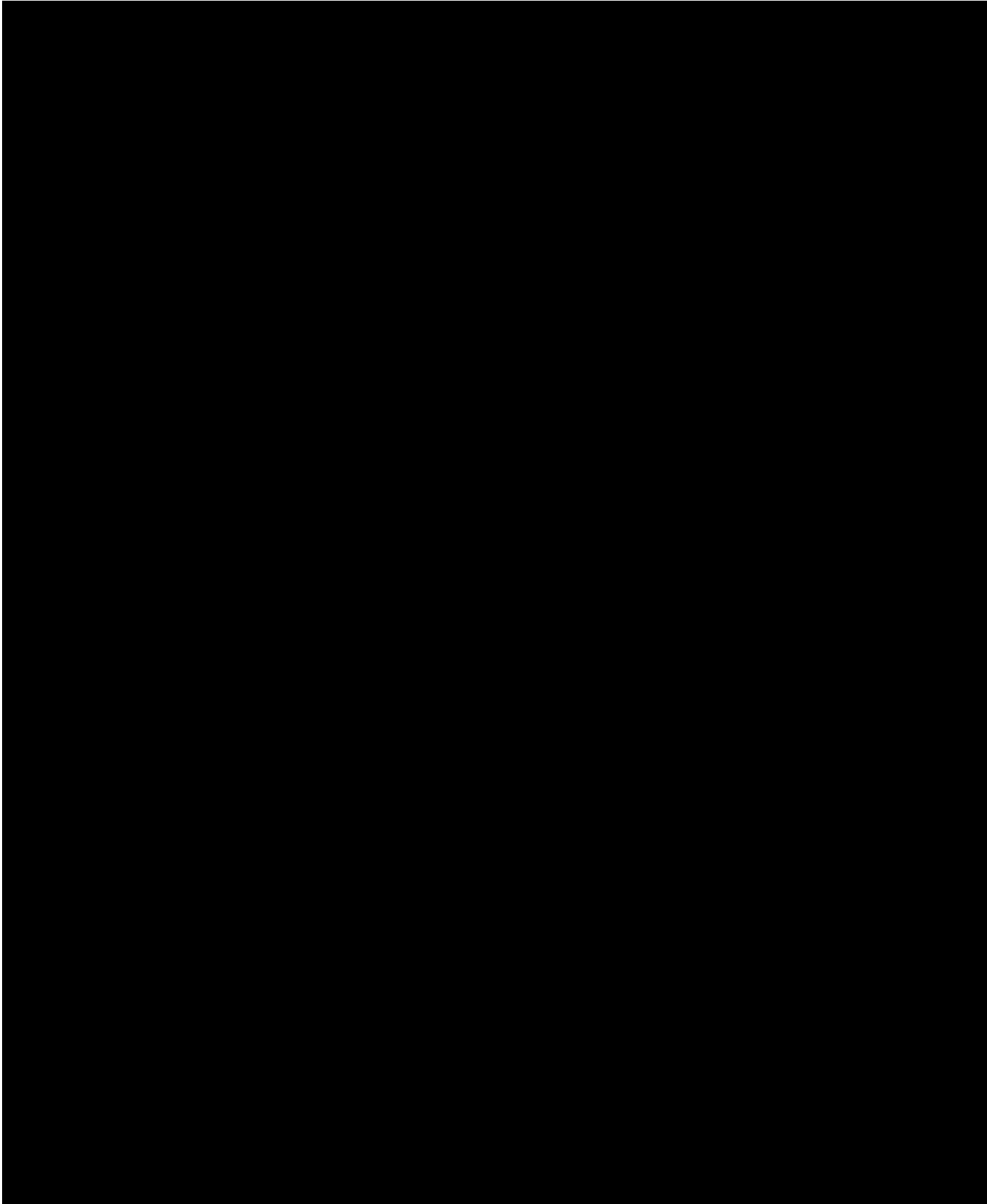


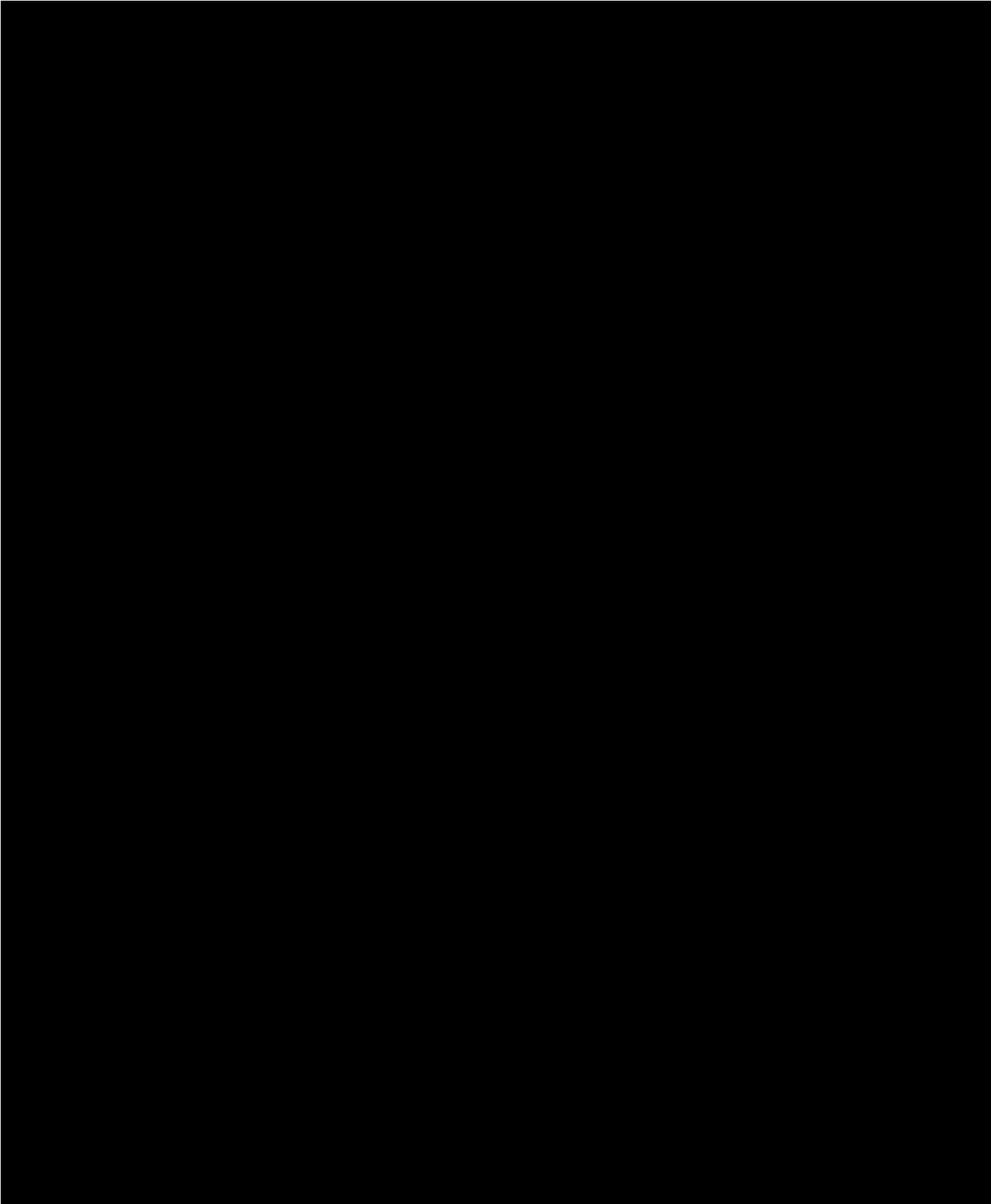


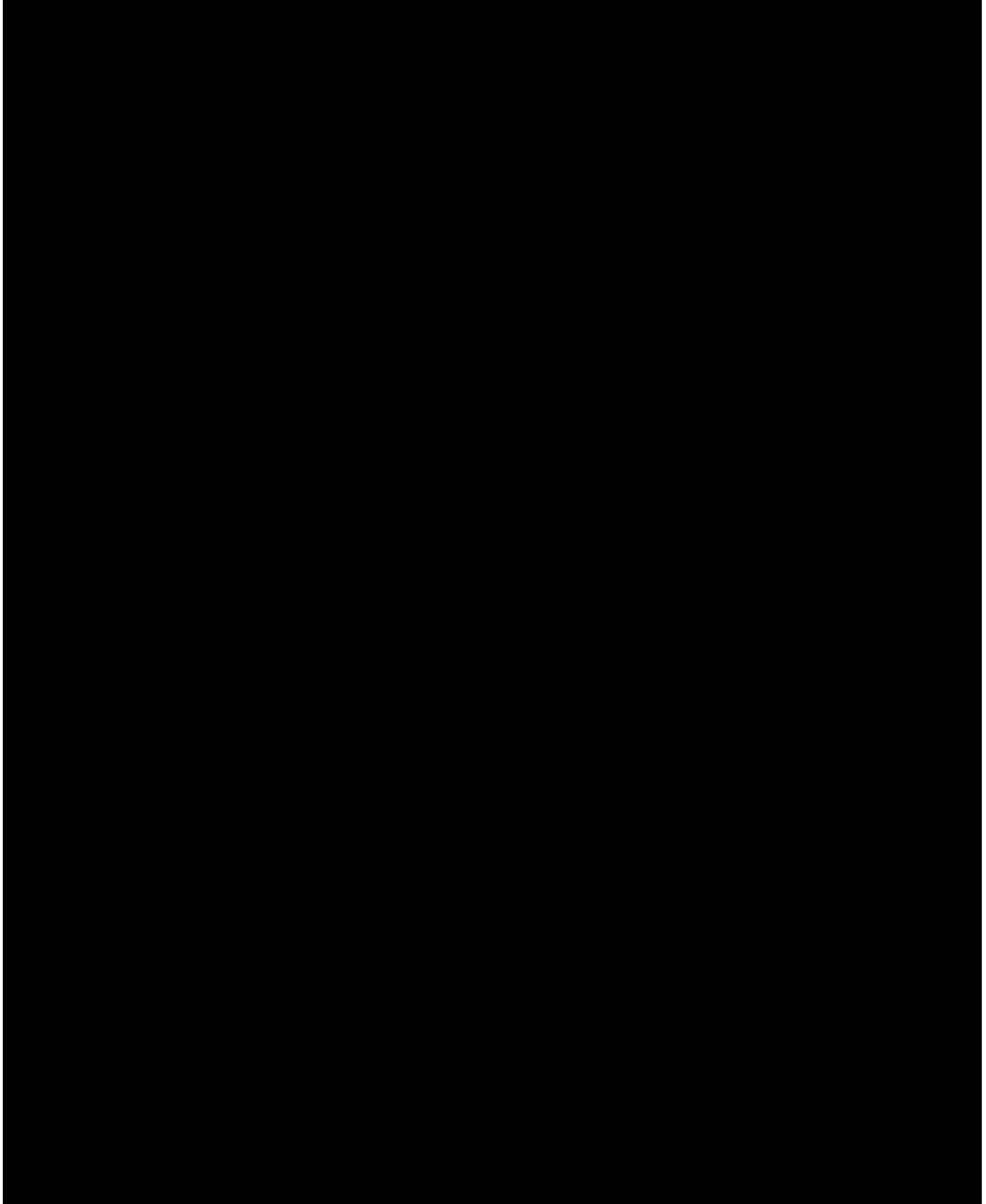


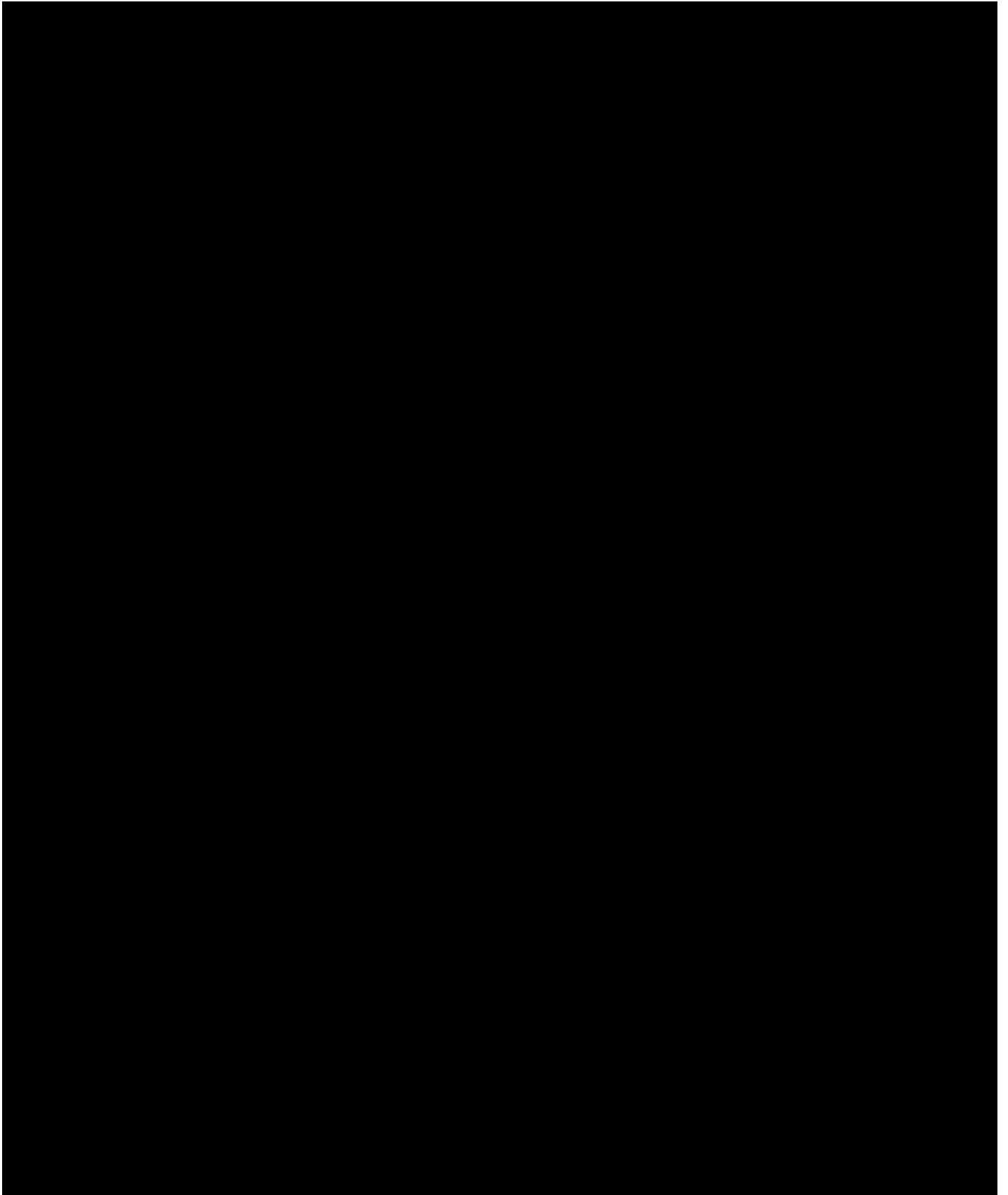


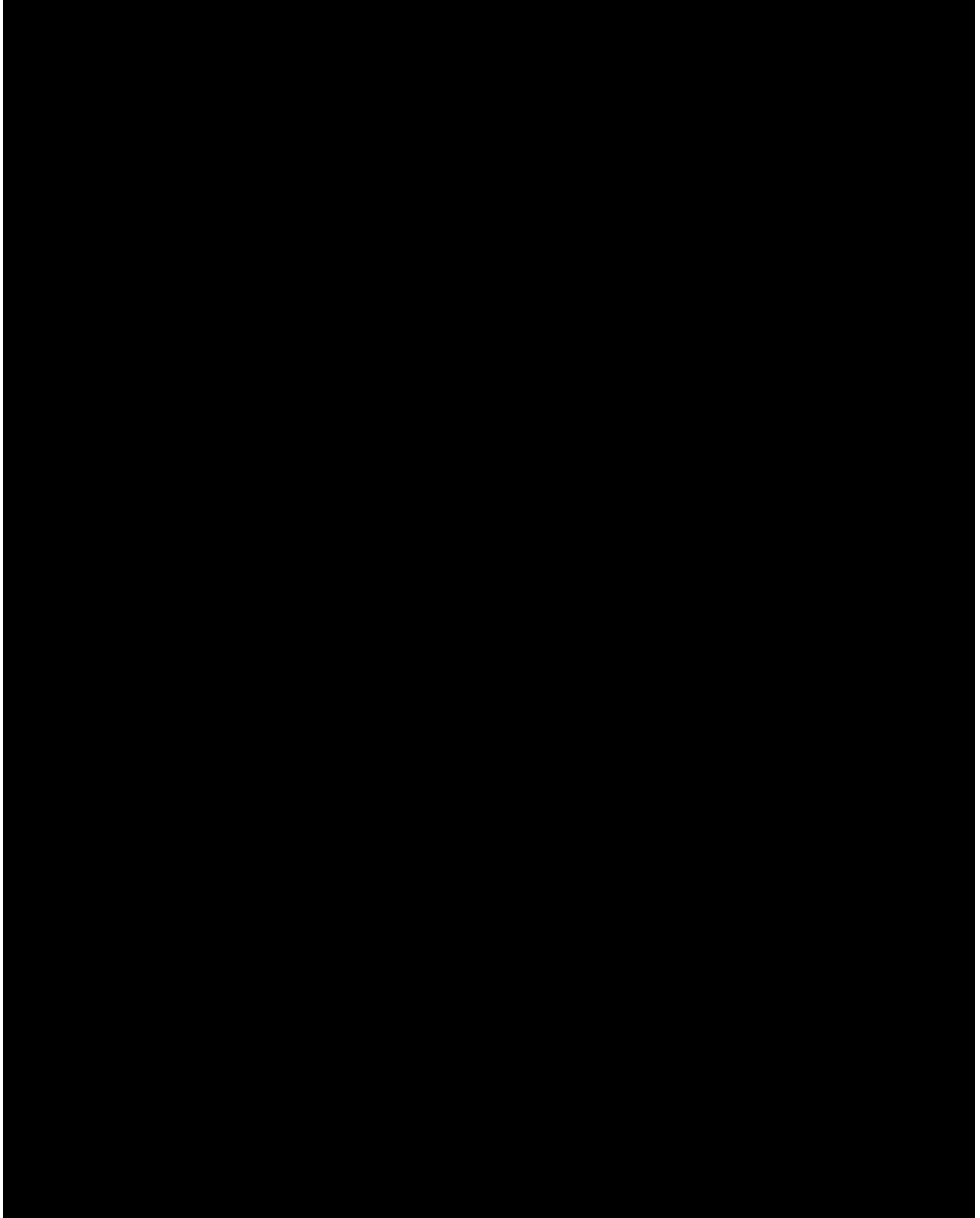












FOR OFFICIAL USE ONLY

**HIGHLY CONFIDENTIAL
NOT FOR PUBLIC INSPECTION**

Making materially false, fictitious, or fraudulent statements or representations may render the Applicant subject to fines and/or imprisonment under 18 U.S.C. § 1001.

I declare that the foregoing is true and correct to the best of my knowledge.

Executed this 27 day of April, year of 2012.

X


b1. (Applicant Signature) Director, Zhenhui LIN

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 4

EXHIBIT A



EXHIBIT B



EXHIBIT C

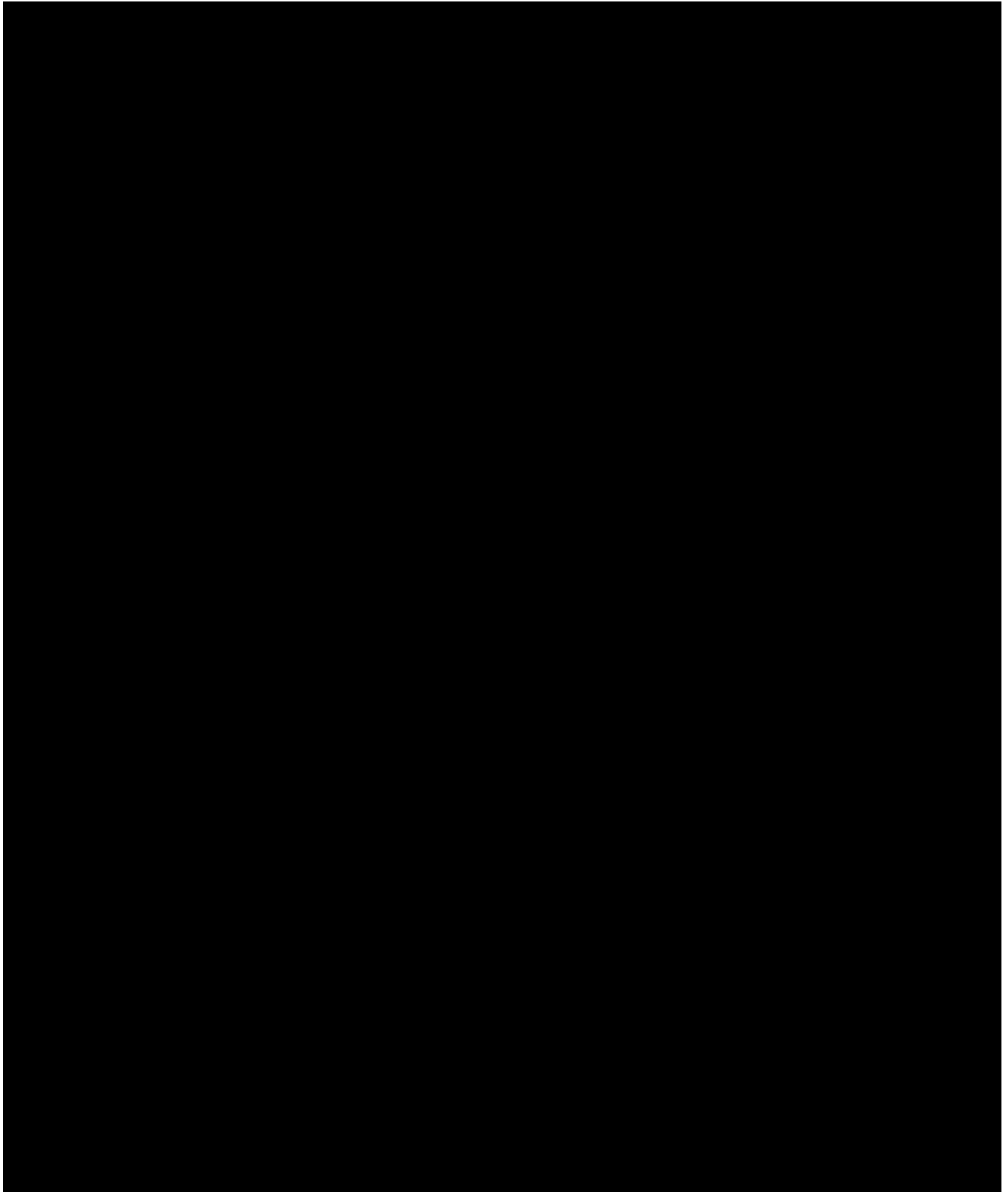
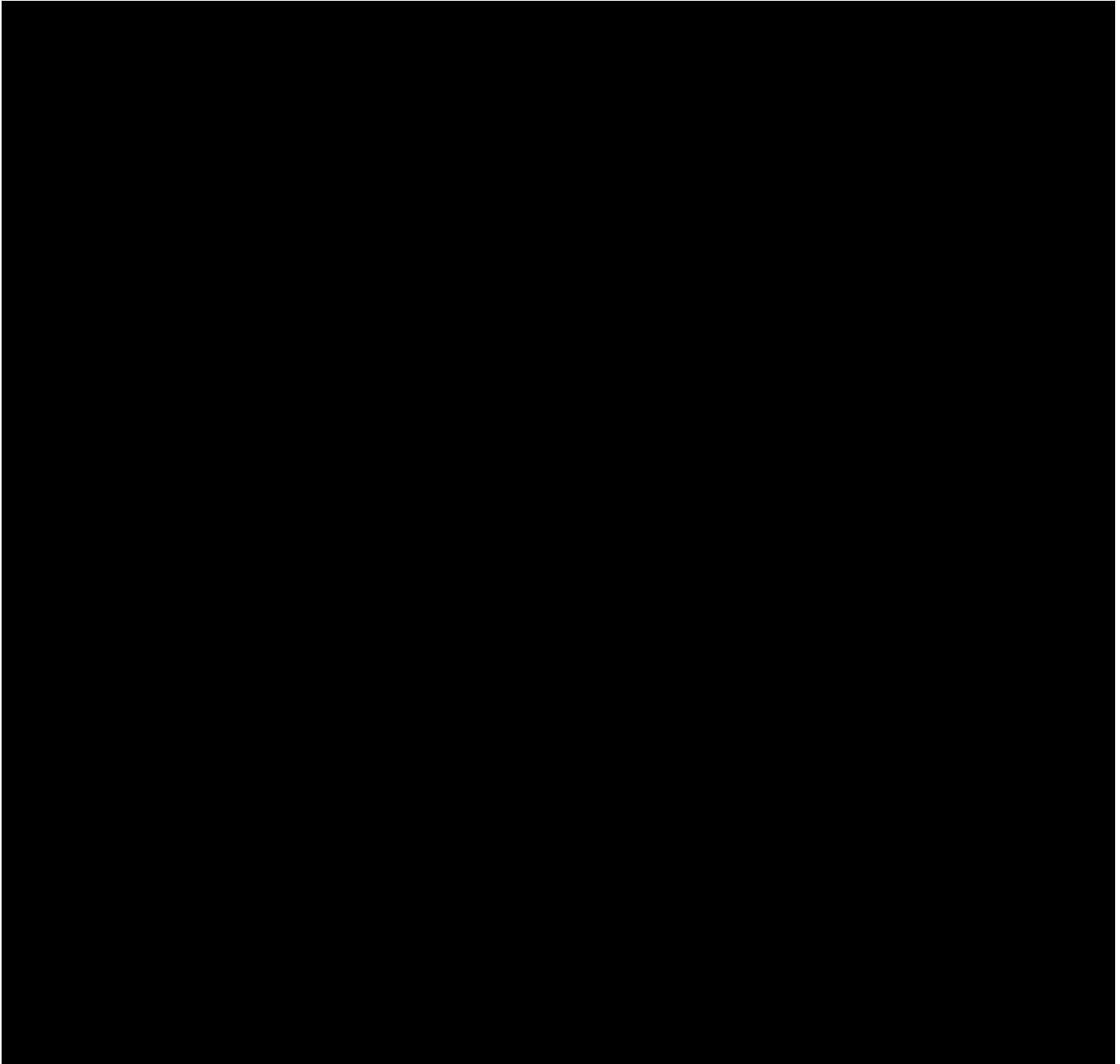


EXHIBIT D



EXHIBIT E



**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 5

WILKINSON) BARKER) KNAUER) LLP

2300 N STREET, NW
SUITE 700
WASHINGTON, DC 20037
TEL 202.783.4141
FAX 202.783.5851
WWW.WBKLaw.COM
JENNIFER L. KOSTYU
DIRECT 202.383.3384
JKOSTYU@WBKLaw.COM

October 7, 2013

VIA EMAIL

Team Telecom
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530
Attn: Tyrone Brown

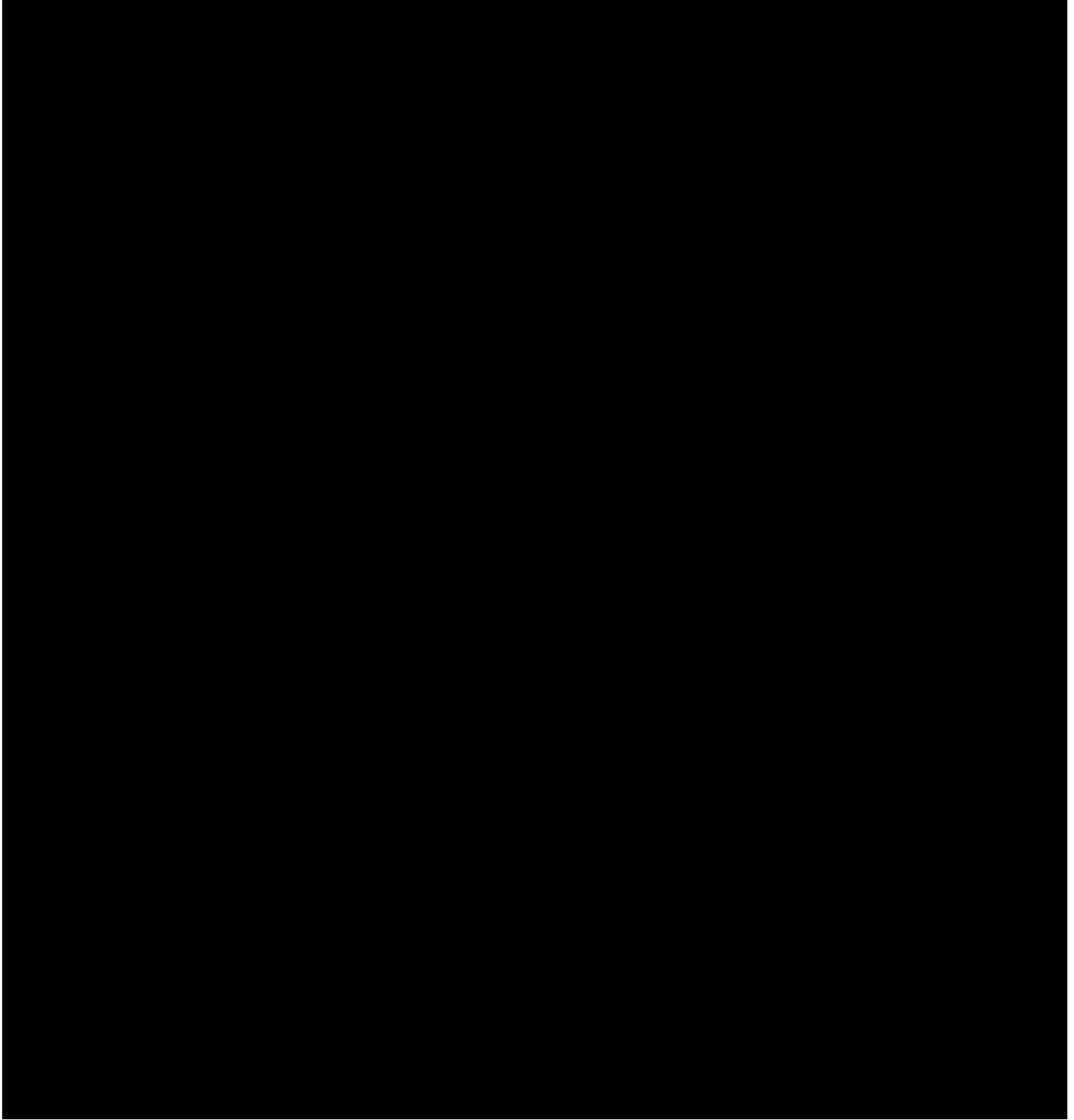
Re: *China Mobile International (USA) Inc. Supplement*
FCC File No. ITC-214-20110901-00289

Dear Mr. Brown:

China Mobile International (USA) Inc. (“CMI USA”), through its attorneys, follows up on the status of Team Telecom’s review relating to the above referenced International Section 214 application (the “Application”). Because this letter includes confidential and proprietary information that is highly competitively sensitive, CMI USA requests that it be given confidential treatment in its entirety consistent with the company’s prior submissions pursuant to Section 552(b)(4) of the Freedom of Information Act.¹

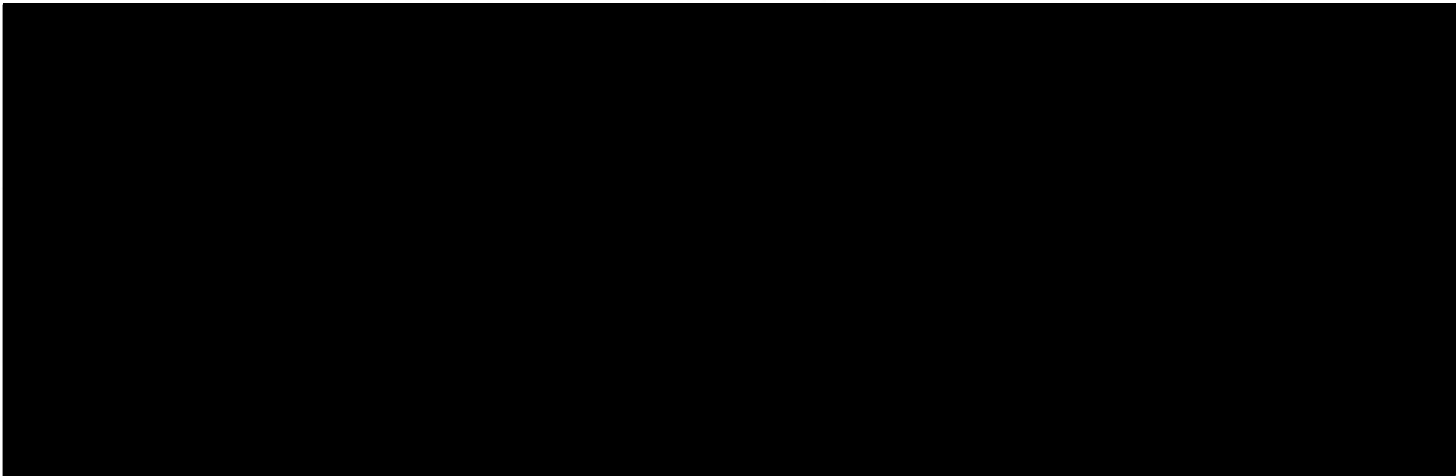
¹ 5 U.S.C. § 552(b)(4). Exemption 4 of the FOIA provides that an agency need not disclose “trade secrets and commercial or financial information obtained from a person which is privileged or confidential.”

Tyrone Brown
October 7, 2013
Page 2



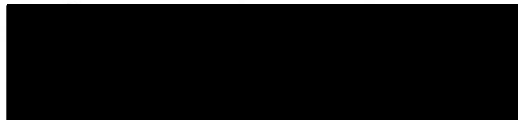
WILKINSON) BARKER) KNAUER) LLP

Tyrone Brown
October 7, 2013
Page 3



If you have any questions regarding the information set forth above, please contact the undersigned.

Very truly yours,



Jennifer L. Kostyu
Counsel to China Mobile International (USA) Inc.

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 6



HARRIS, WILTSHIRE
& GRANNIS LLP

1919 M STREET NW
SUITE 800
WASHINGTON DC 20036

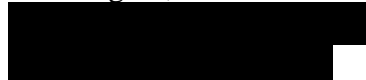
TEL +1 202 730 1300
FAX +1 202 730 1301
HWGLAW.COM

ATTORNEYS AT LAW

25 September 2014

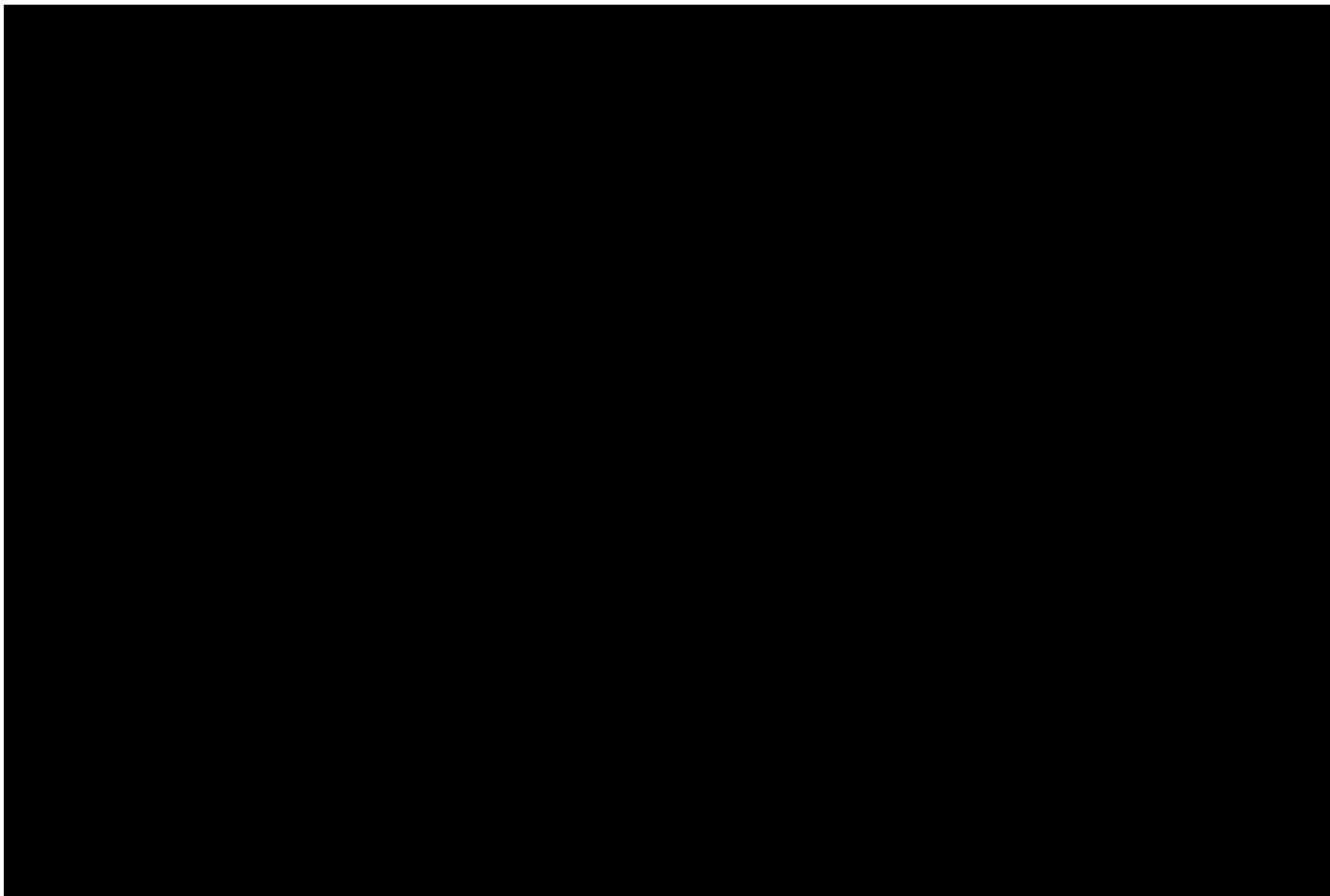
BY ELECTRONIC MAIL

Mr. Richard C. Sofield
Mr. Tyrone Brown
Foreign Investment Review Staff
National Security Division
U.S. Department of Justice
Washington, D.C. 20530

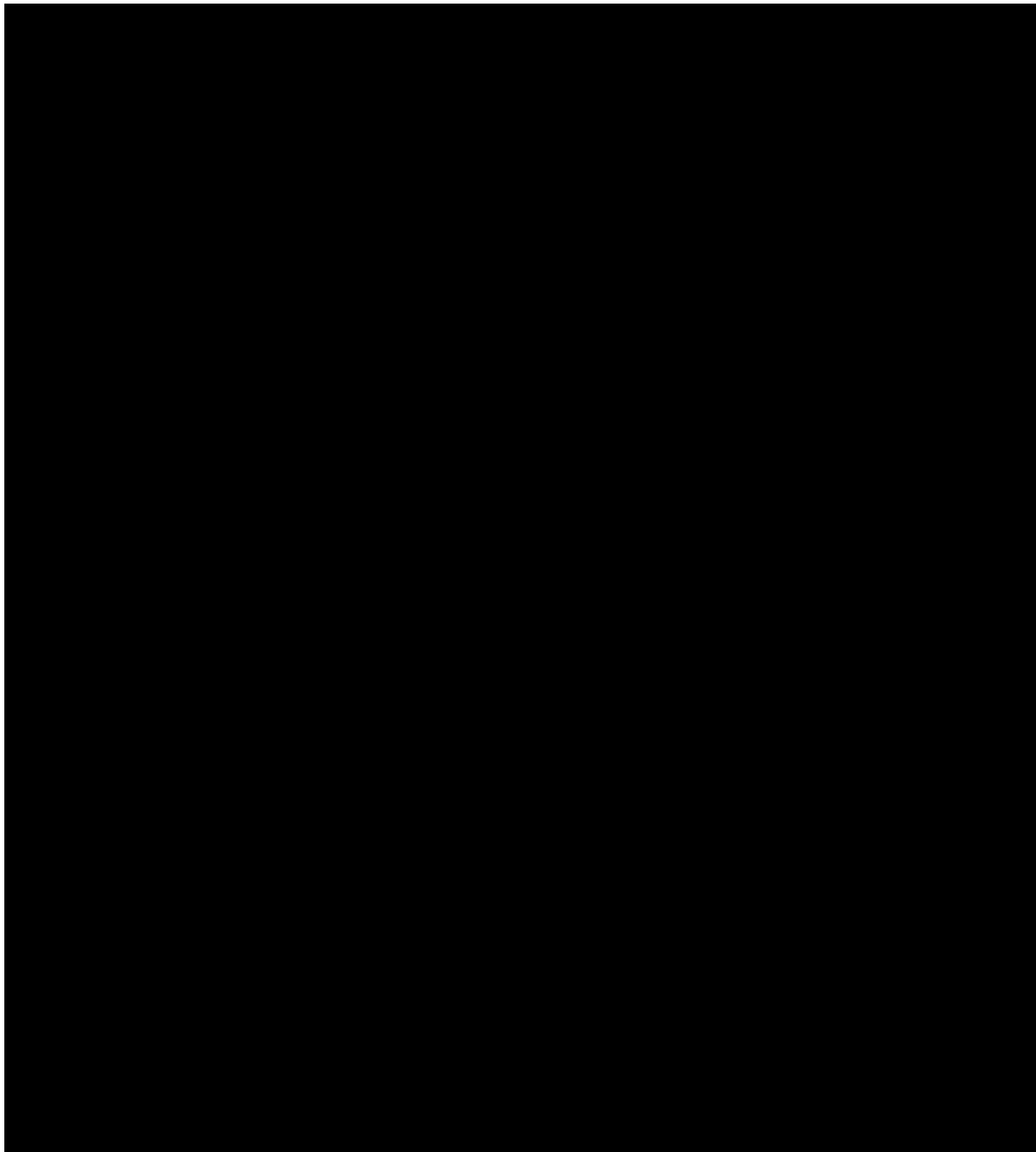


*Re: Application of China Mobile International (USA) Inc. for International Section
214 Authority, FCC File No. ITC-214-20110901-00289*

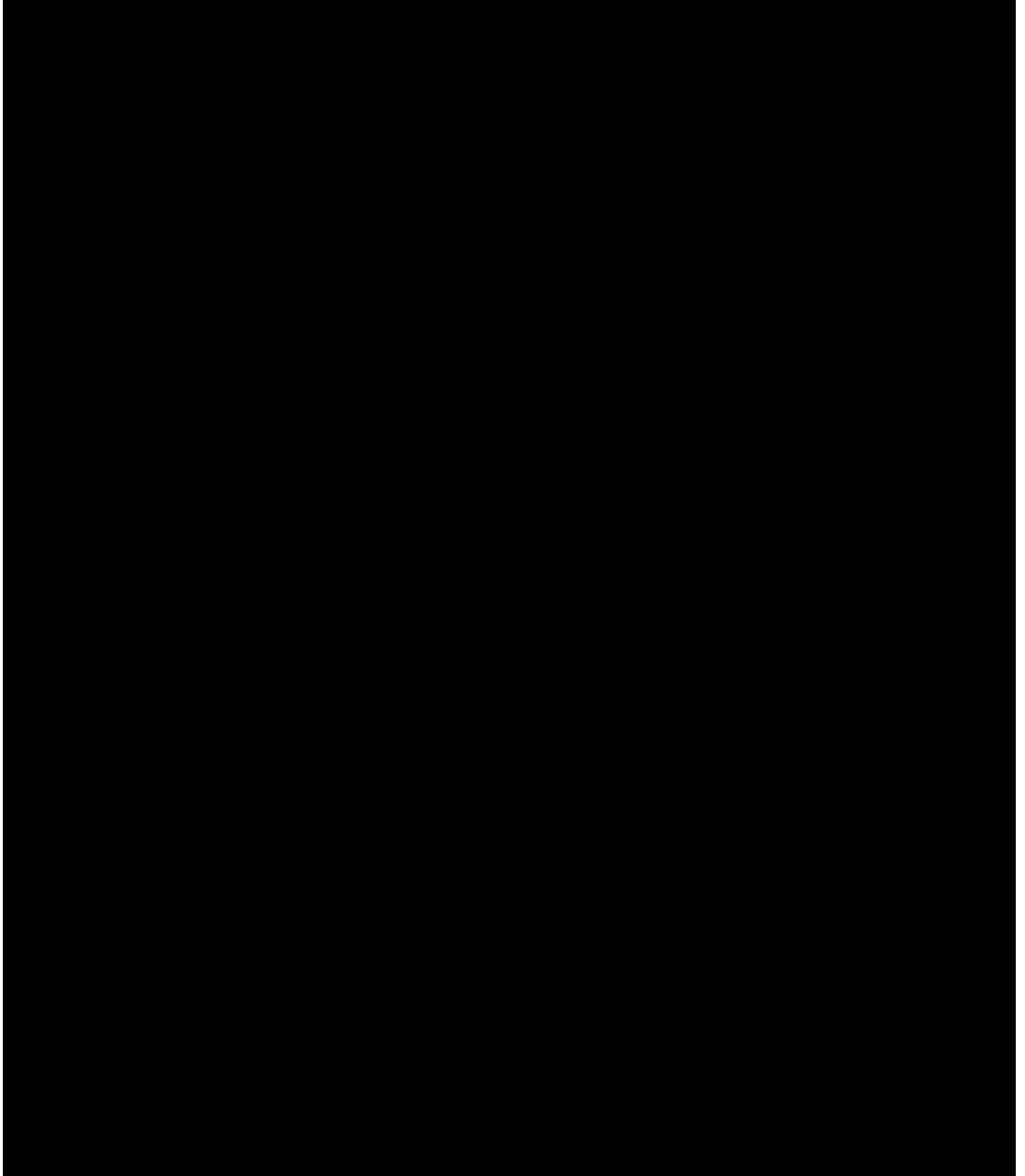
Dear Rick and Ty:



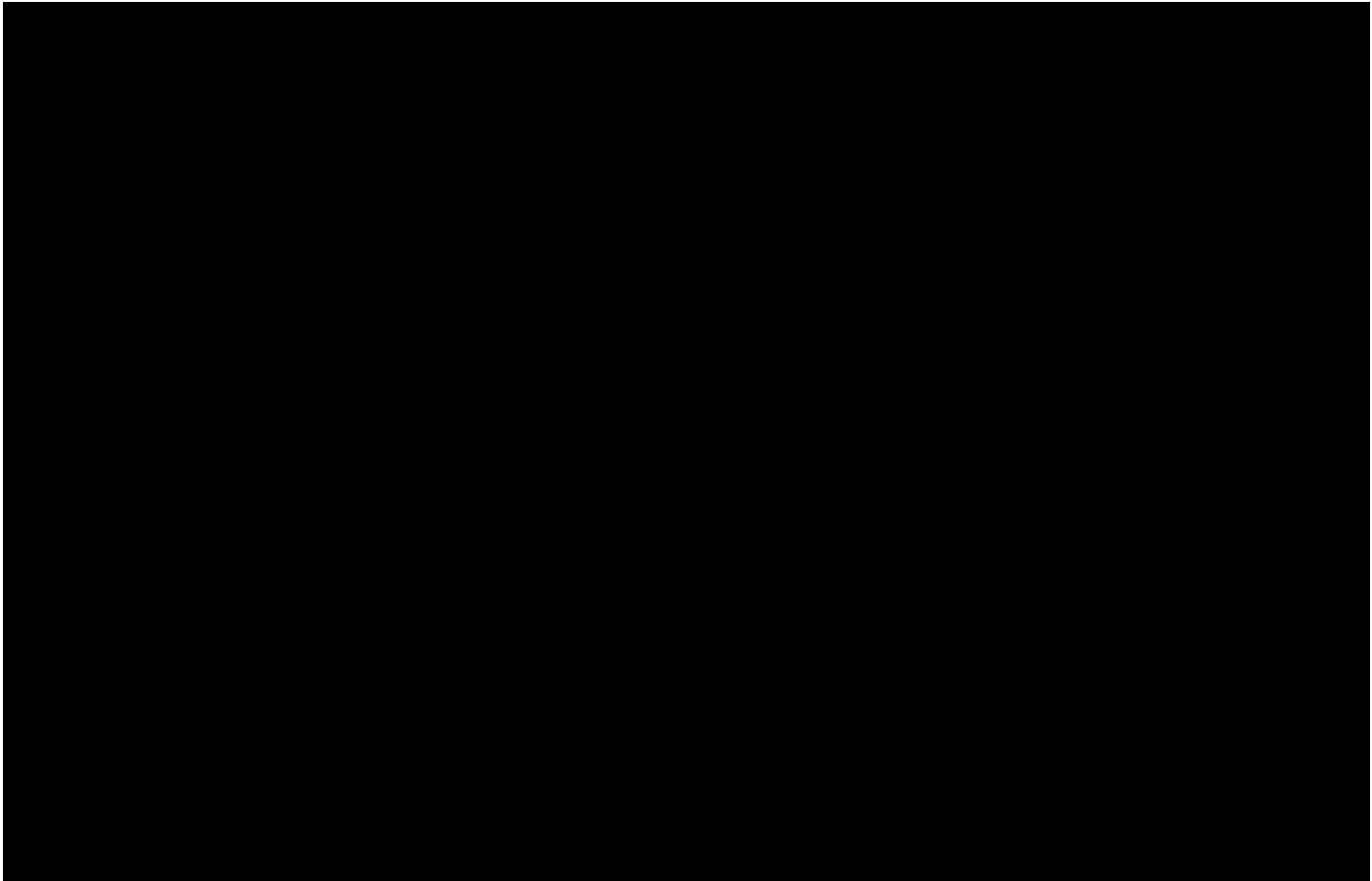
Messrs. Sofield and Brown
U.S. Department of Justice
25 September 2014
Page 2



Messrs. Sofield and Brown
U.S. Department of Justice
25 September 2014
Page 3



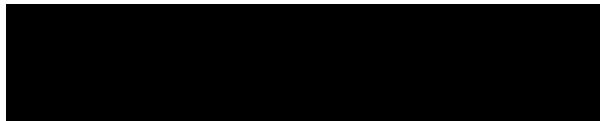
Messrs. Sofield and Brown
U.S. Department of Justice
25 September 2014
Page 4



* * * * *

Should you have additional questions, please do not hesitate to contact Kent Bressie by telephone at +1 202 [REDACTED] or by e-mail at [REDACTED].

Yours sincerely,



Kent Bressie
Patricia Paoletta
Counsel for China Mobile International (USA) Inc.

cc: Team Telecom agencies

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

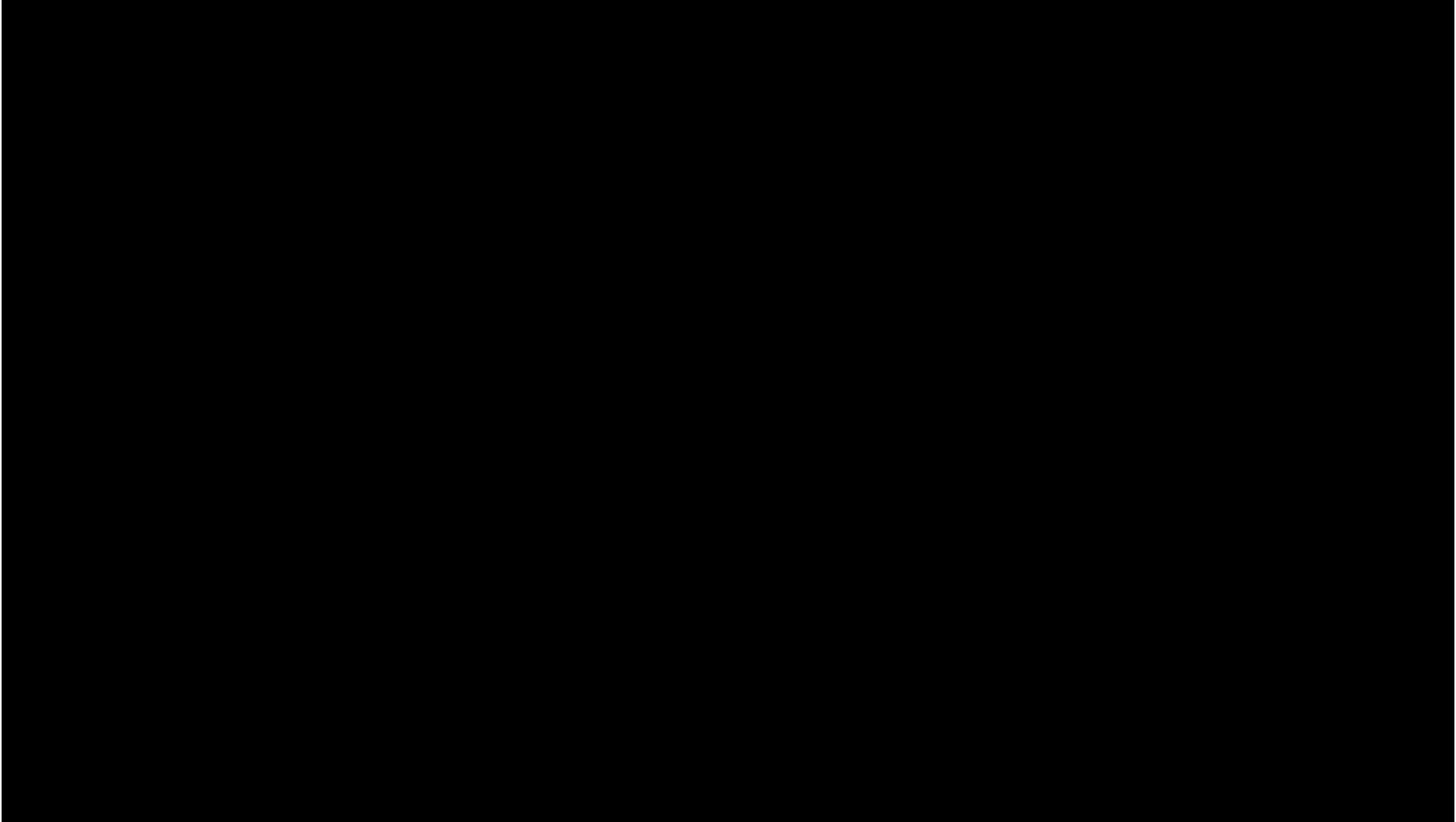
EXHIBIT 7

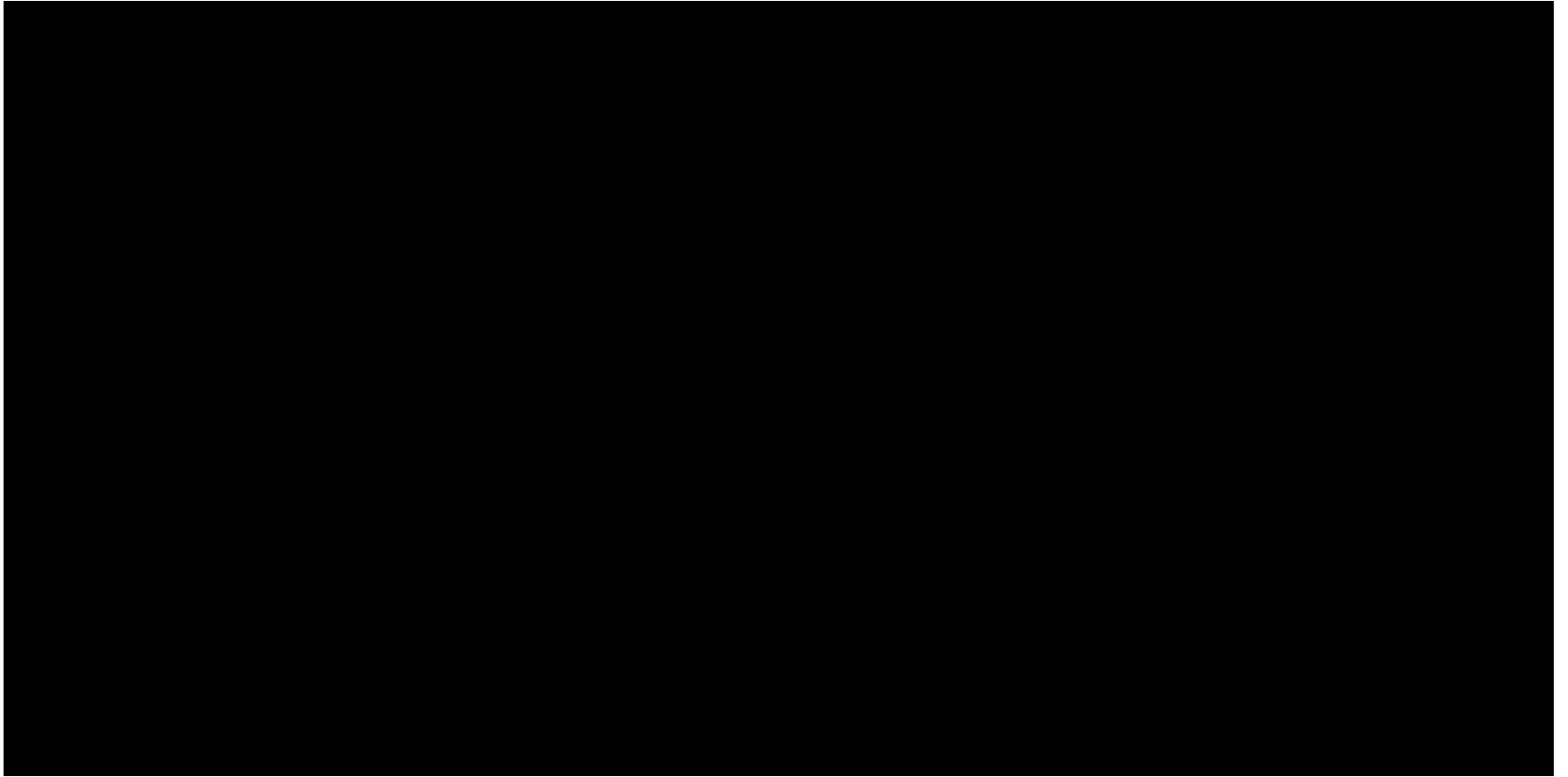
Team Telecom Review of China Mobile International (USA) Inc. Application for Authority from the Federal Communications Commission

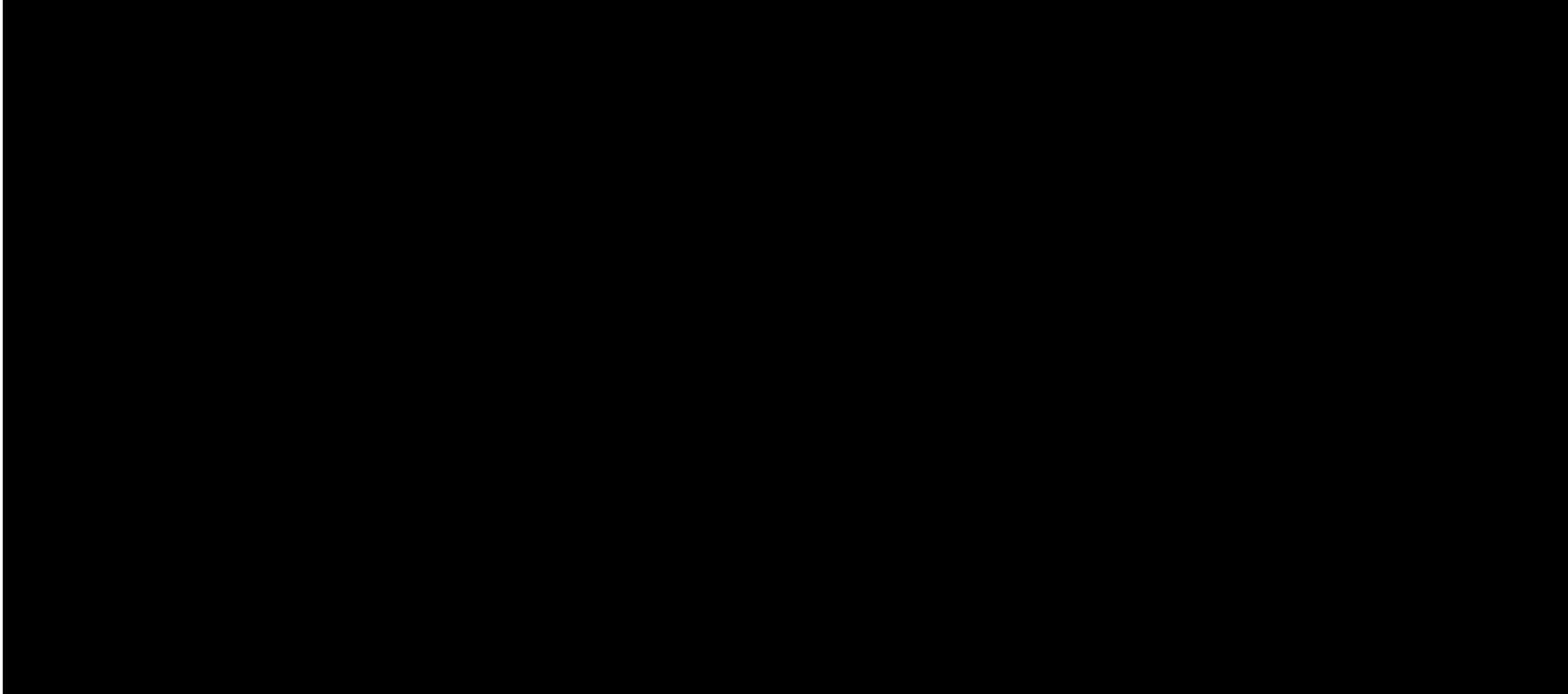
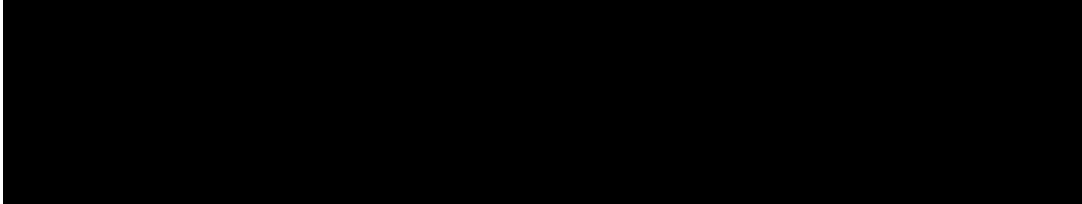
31 October 2014

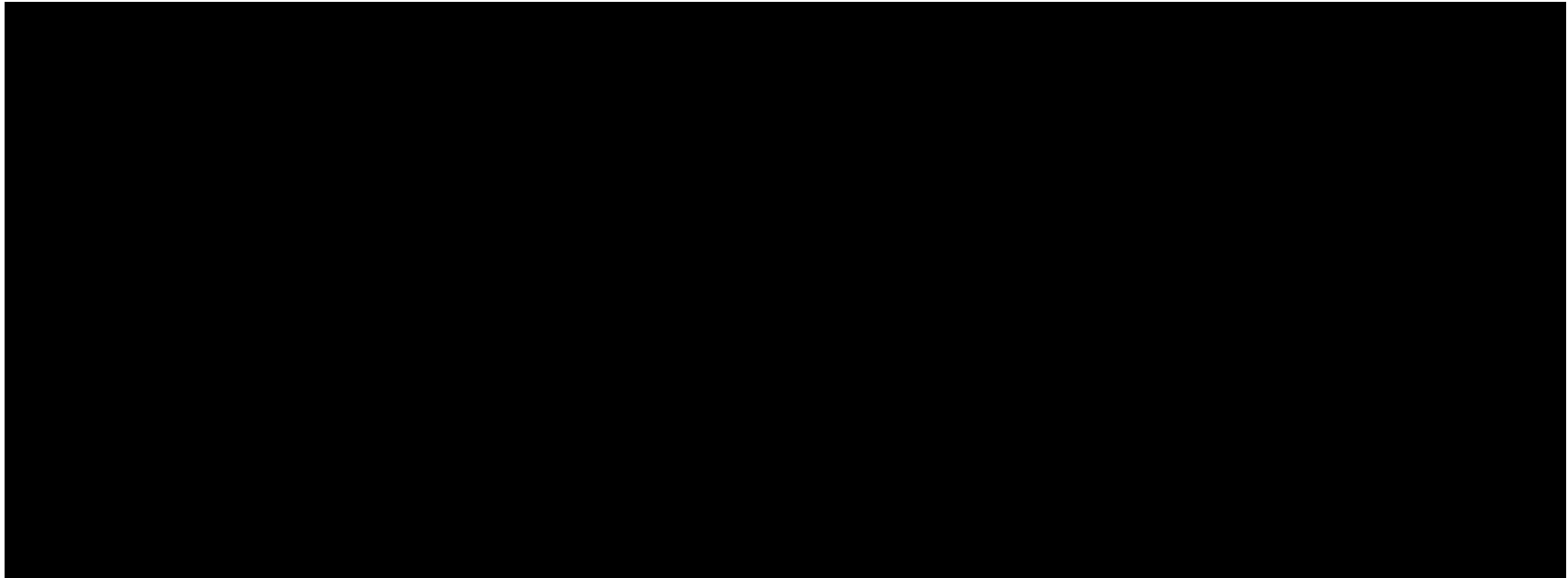
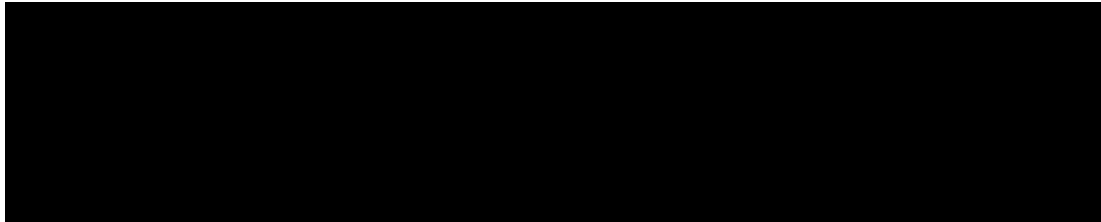
Agenda

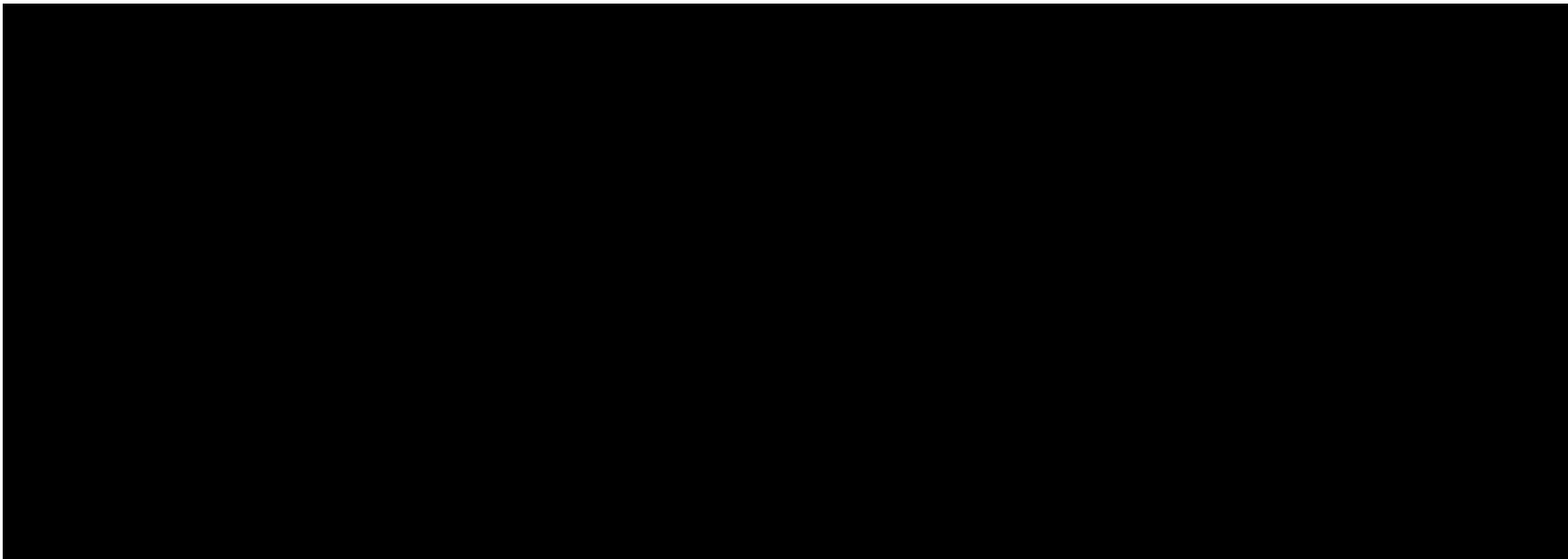
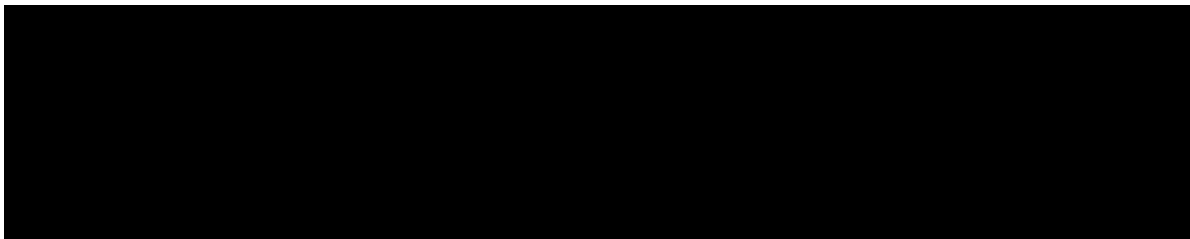
Summary

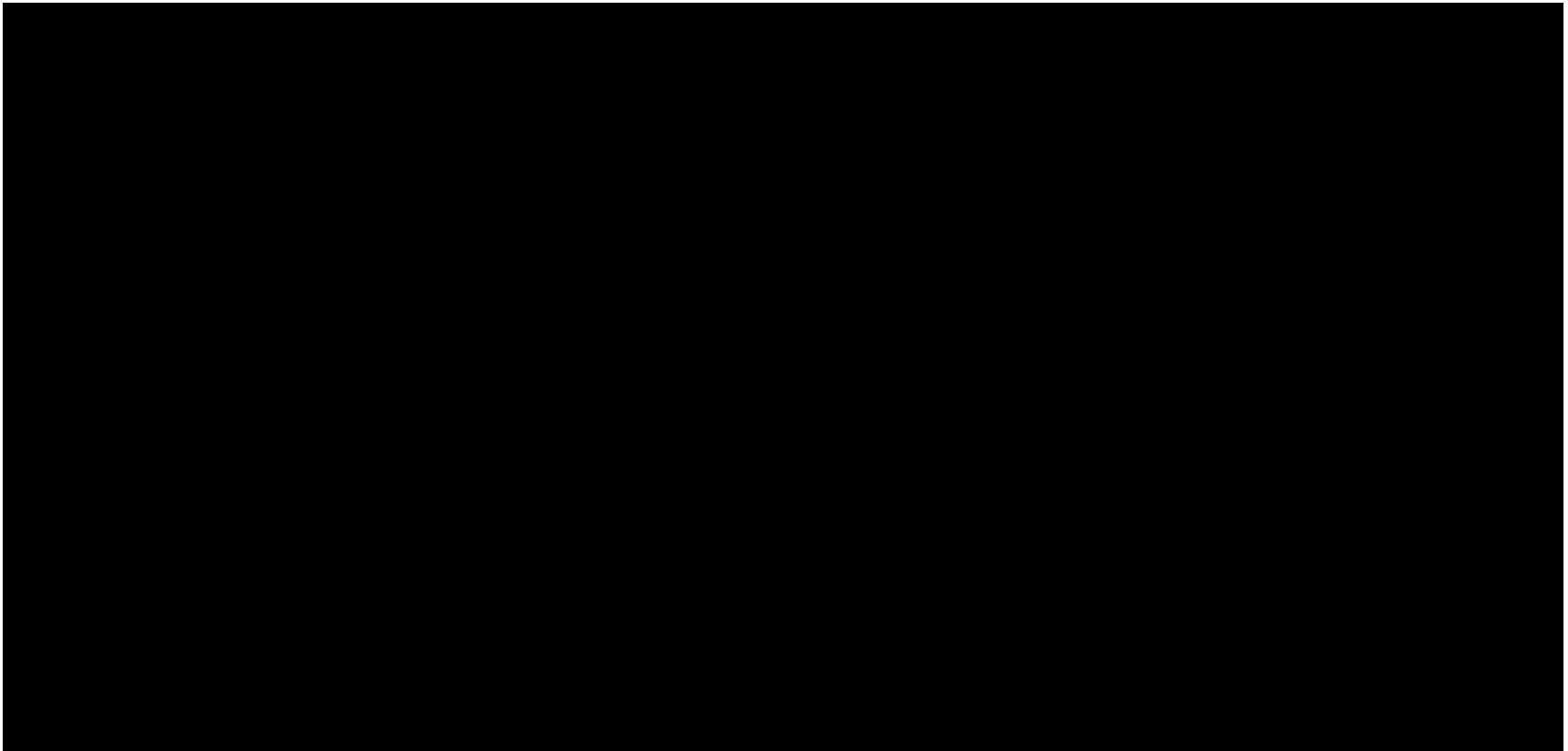
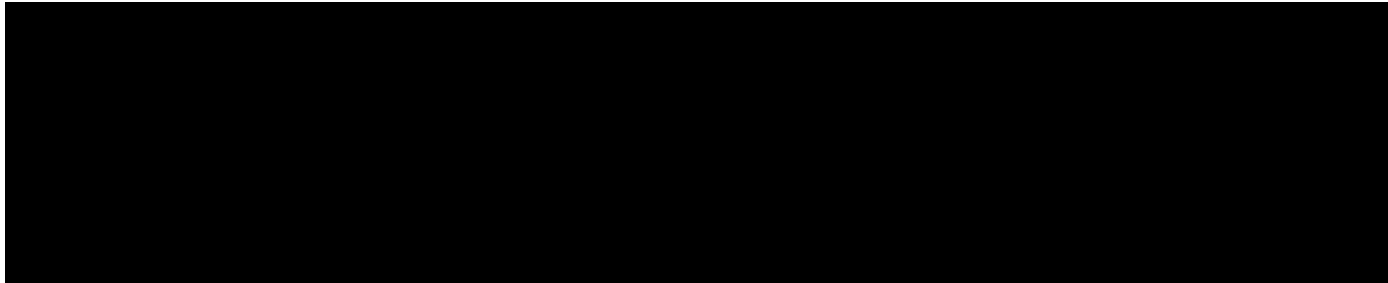




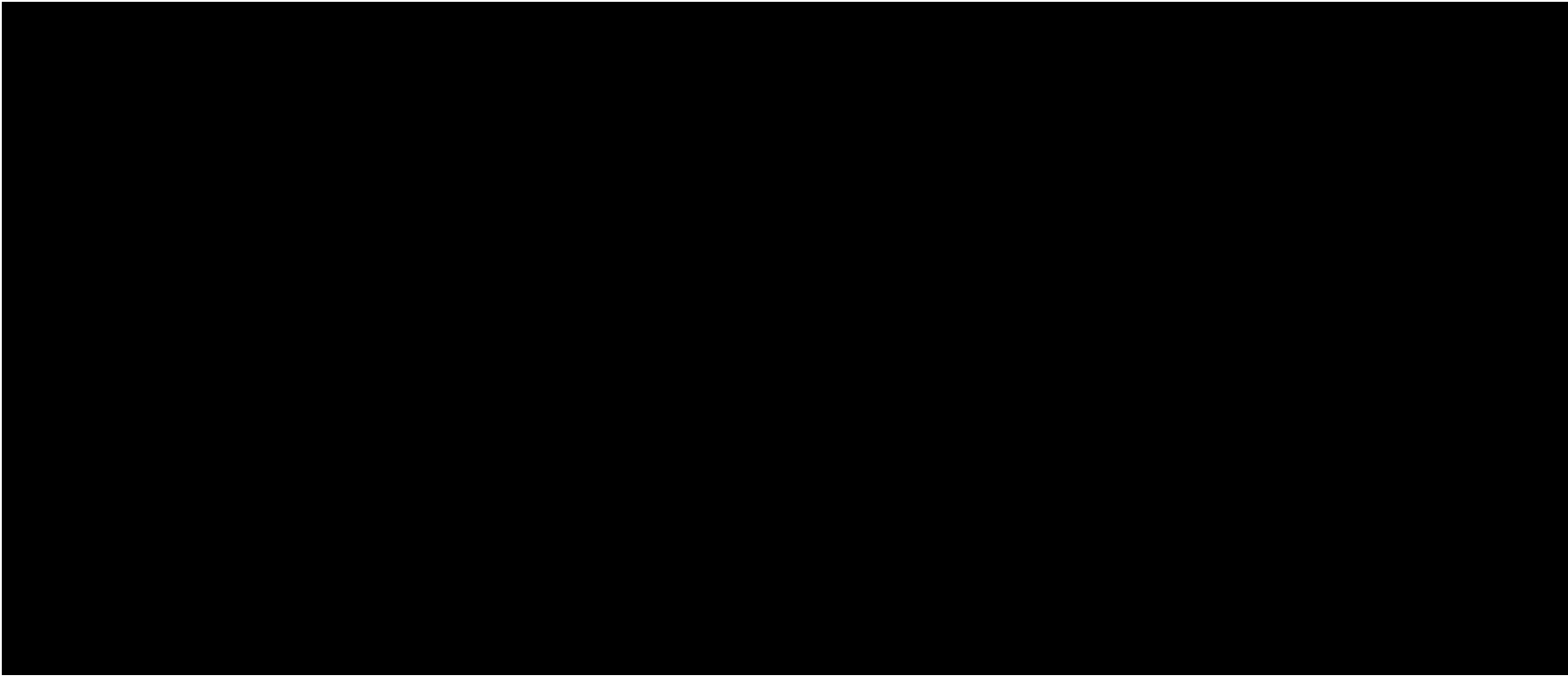
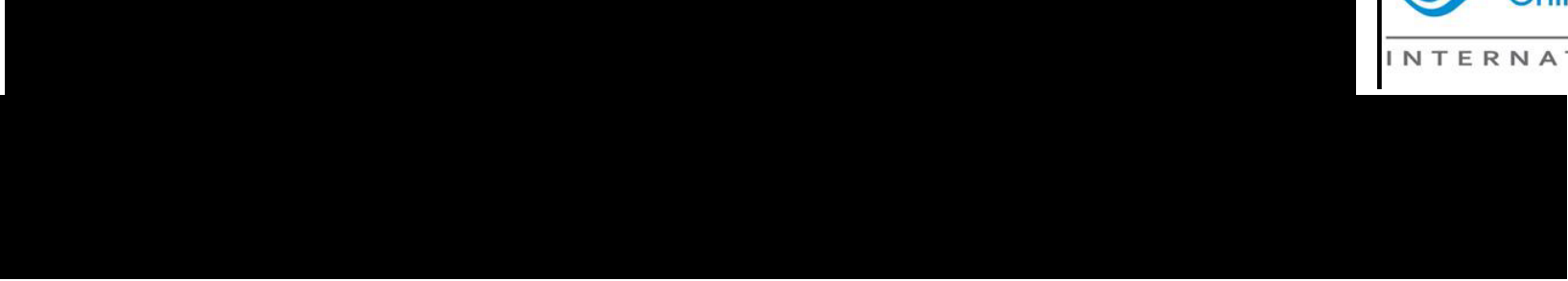


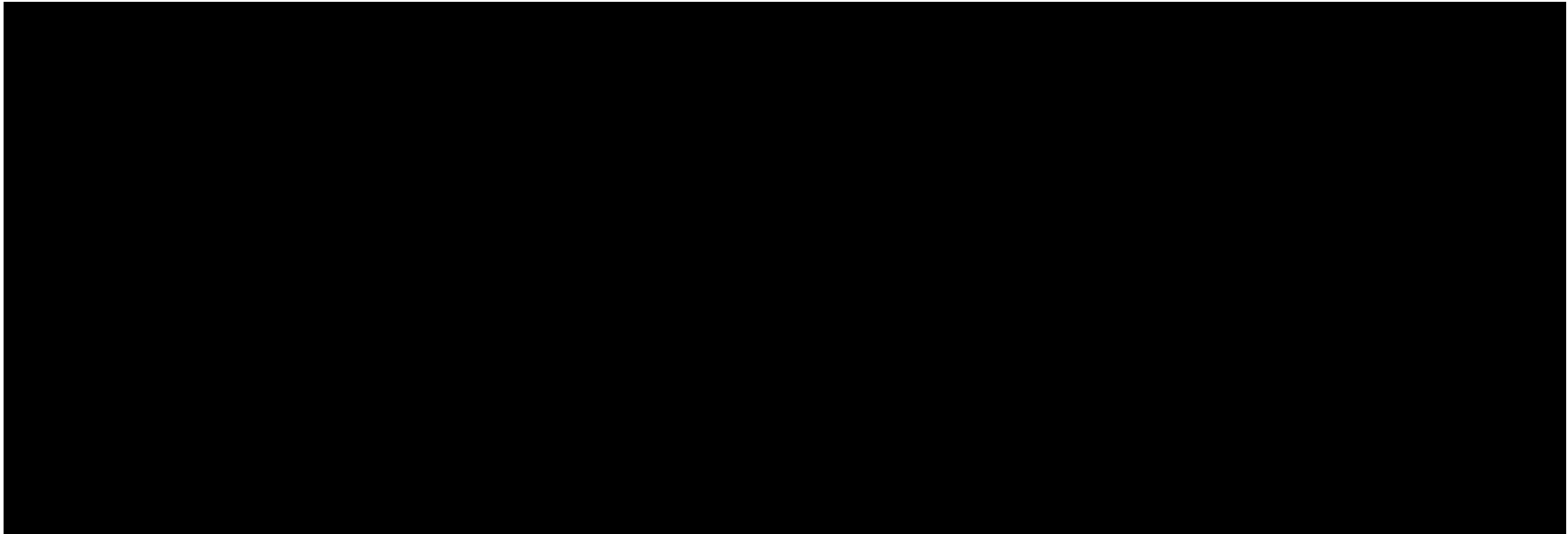
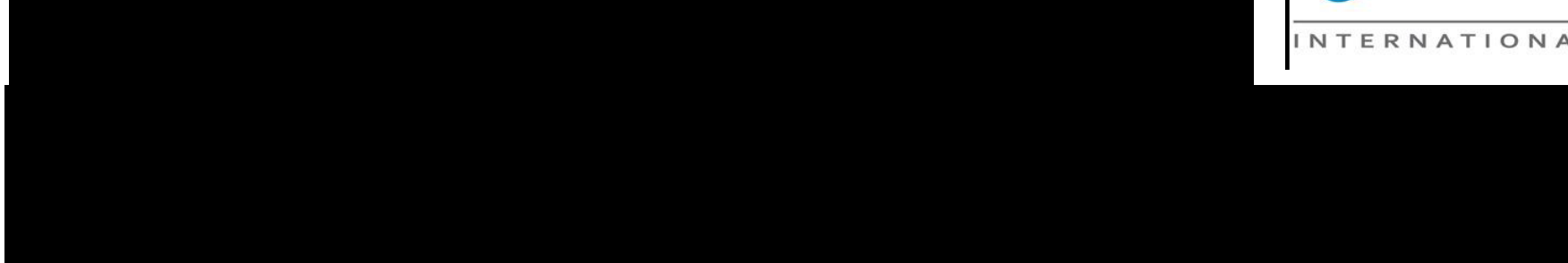


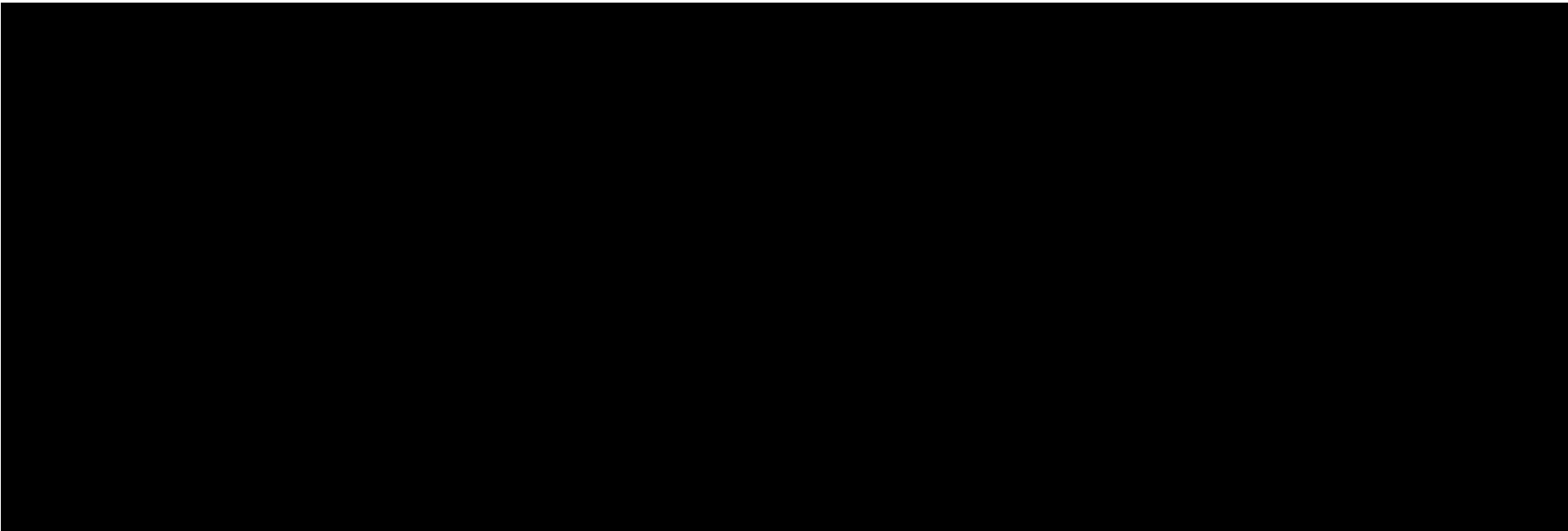
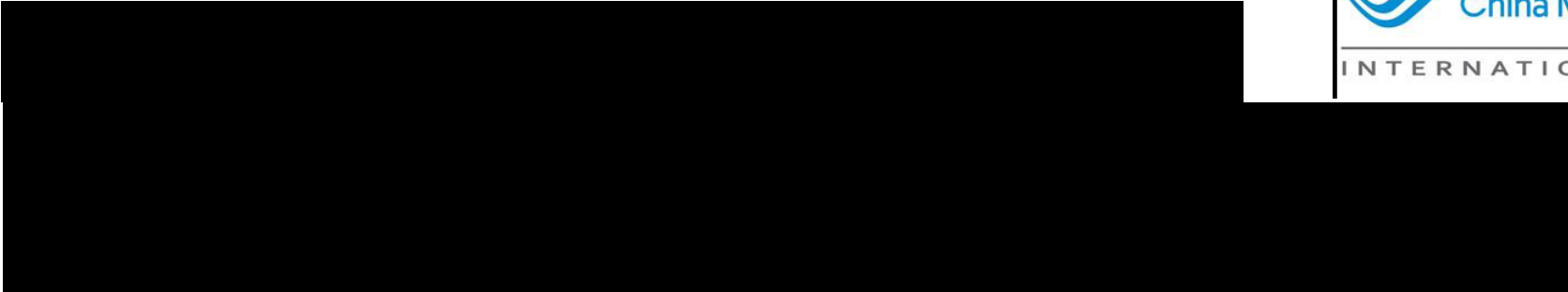


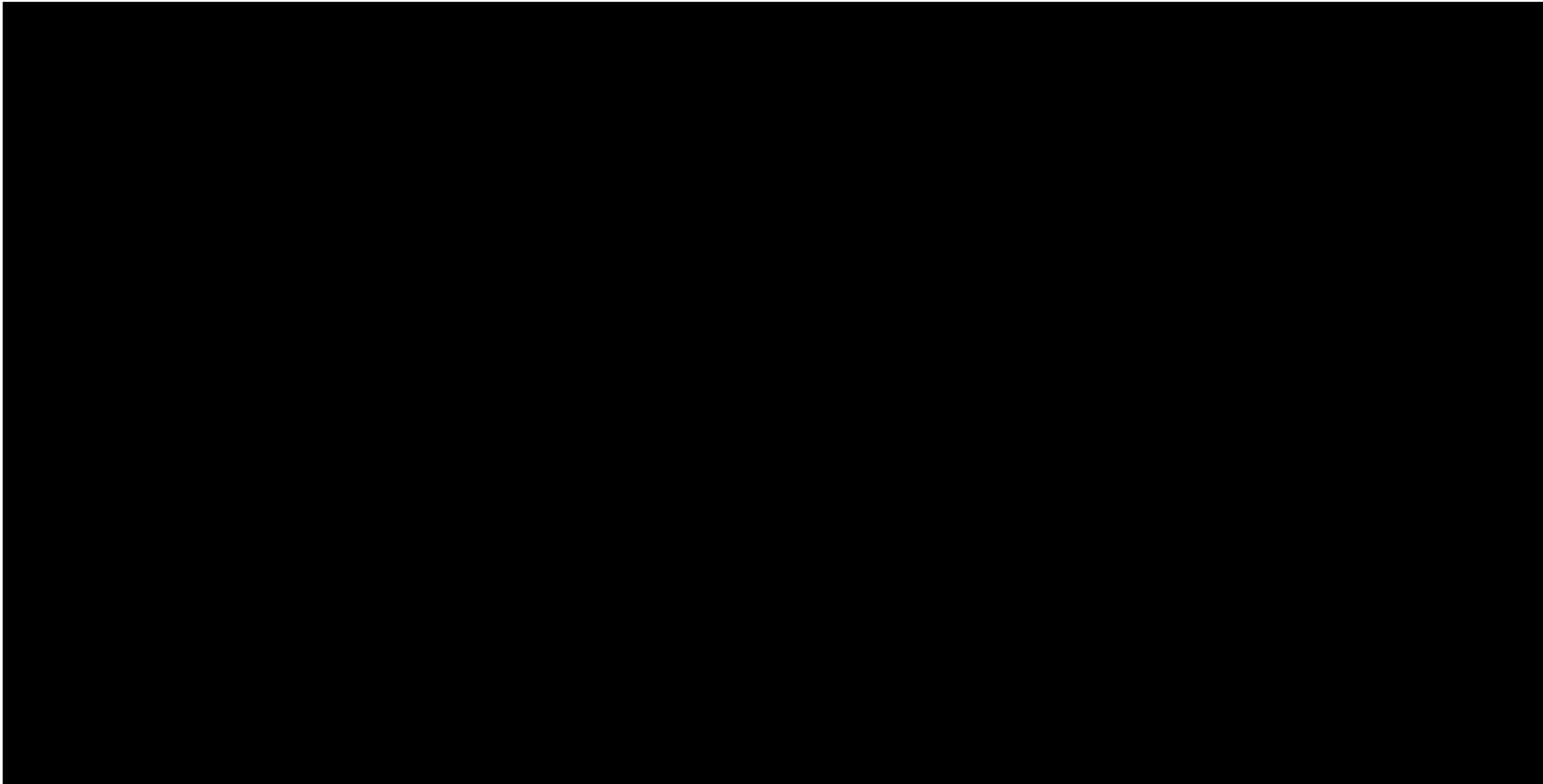
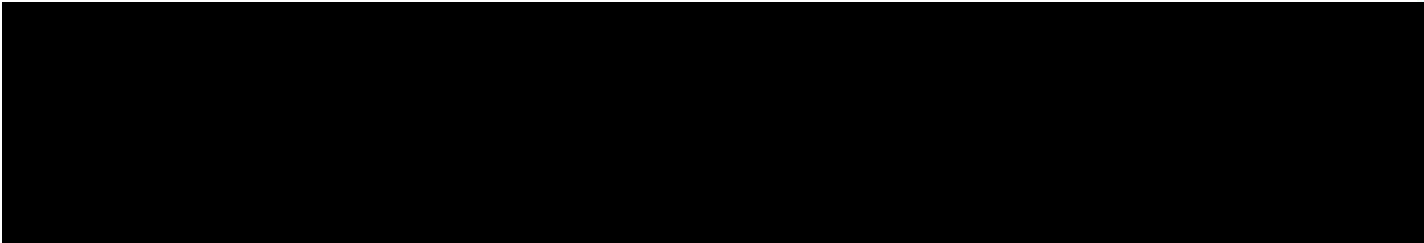


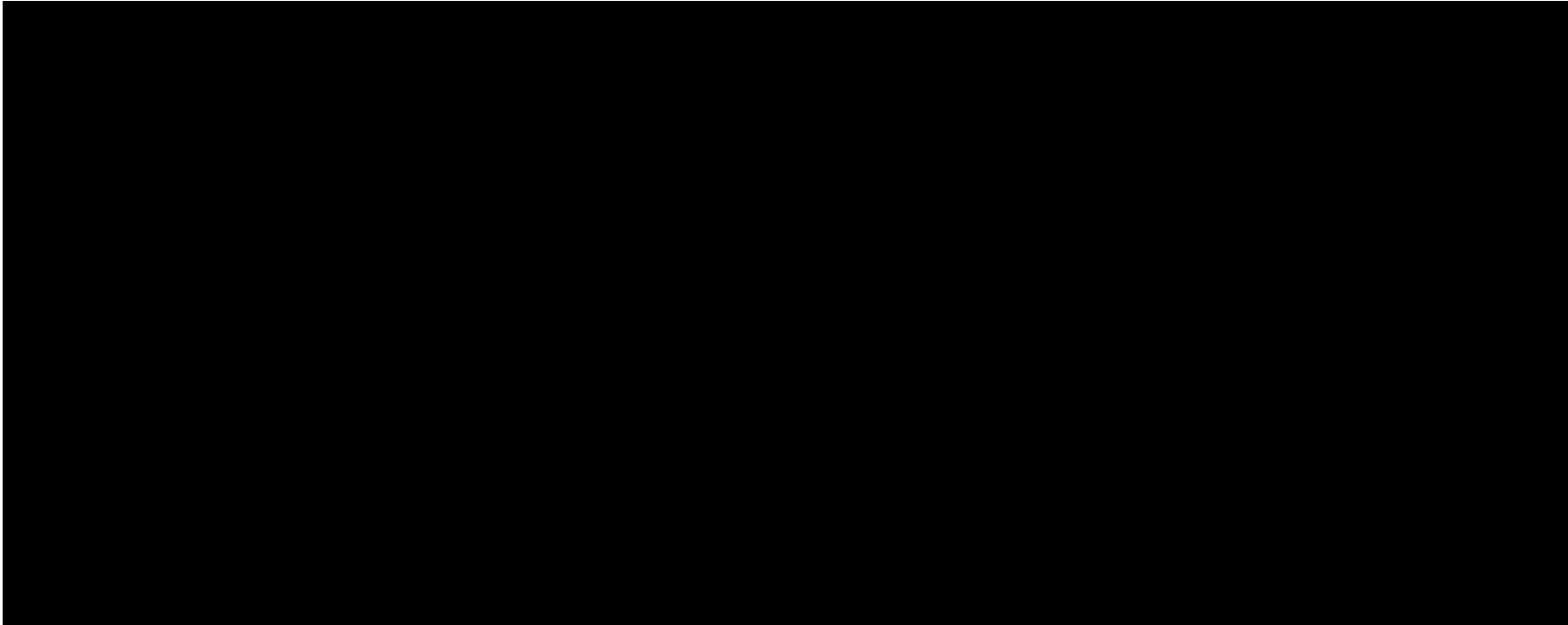
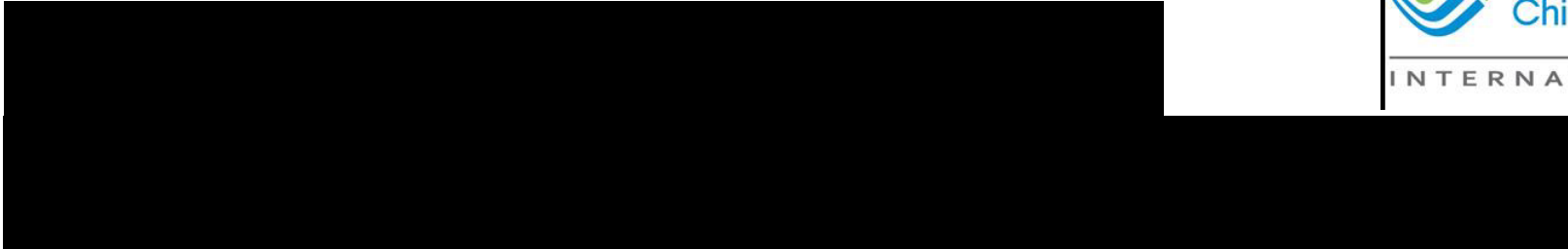












Principal point of contact

Kent Bressie

Harris, Wiltshire & Grannis LLP
1919 M Street, N.W., Suite 800
Washington, D.C. 20036-3537
+1 202 [REDACTED] direct

[REDACTED]
www.hwglaw.com

Counsel for CMIUSA

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 8

Egal, Loyaan (NSD)

Subject: [REDACTED]

From: Kent Bressie [REDACTED]

Sent: Wednesday, January 28, 2015 12:01 PM

To: Juricic, Harry CIV (US) [REDACTED]

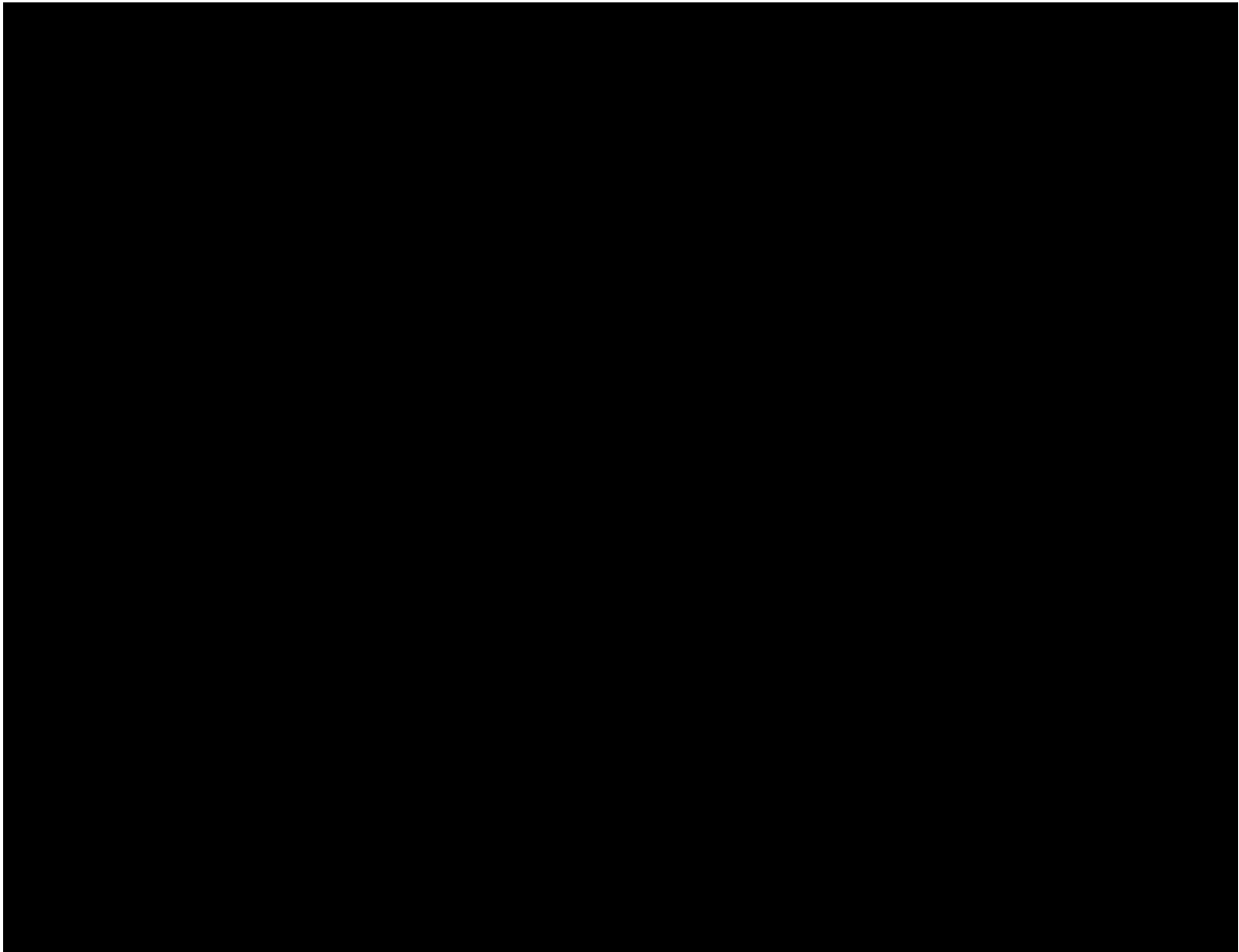
Cc: [REDACTED]; Sofield, Richard (NSD) [REDACTED]; Brown, Tyrone (NSD)

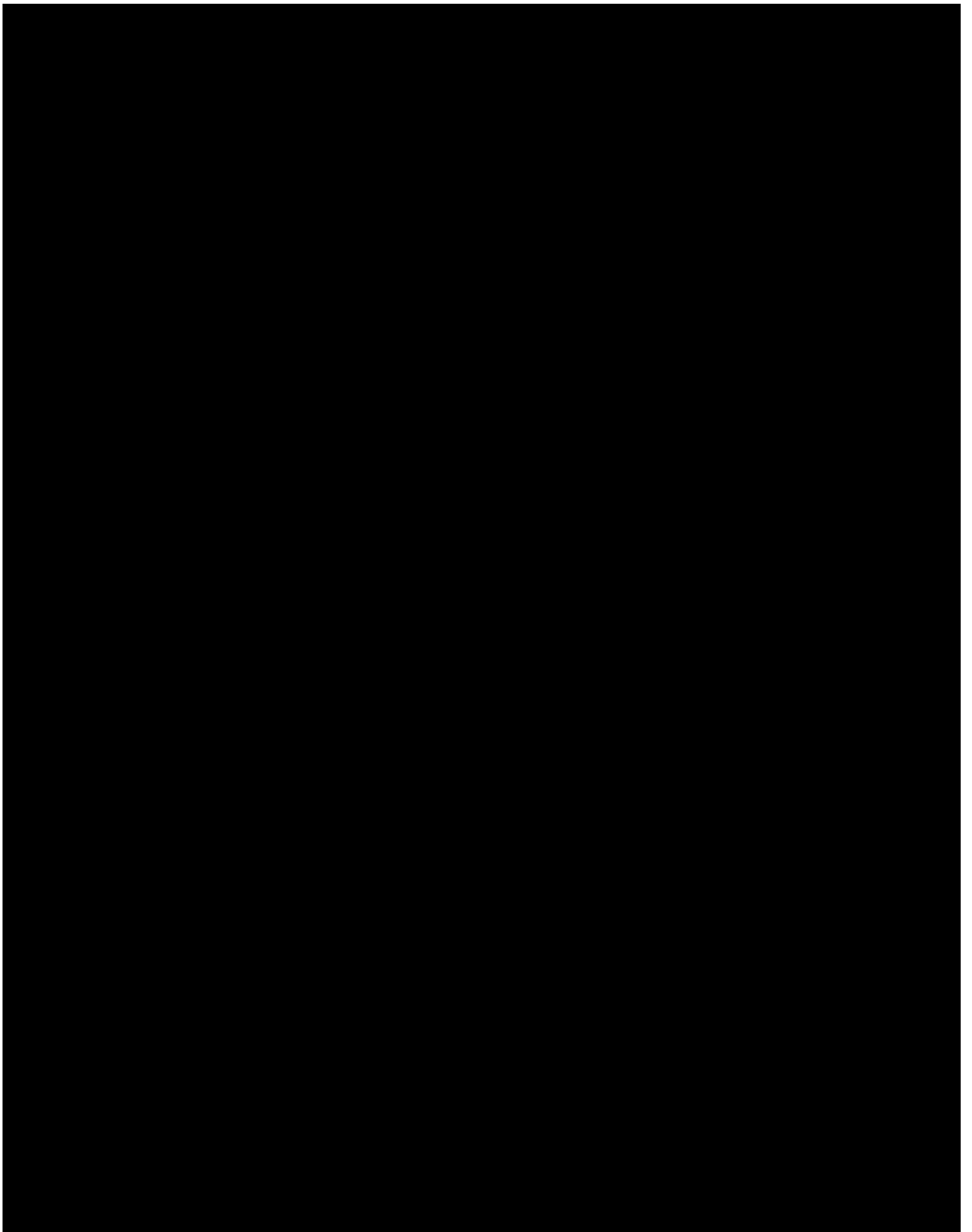
[REDACTED]; Hagar, Richard [REDACTED]; Rosenthal, Daniel (NSD)

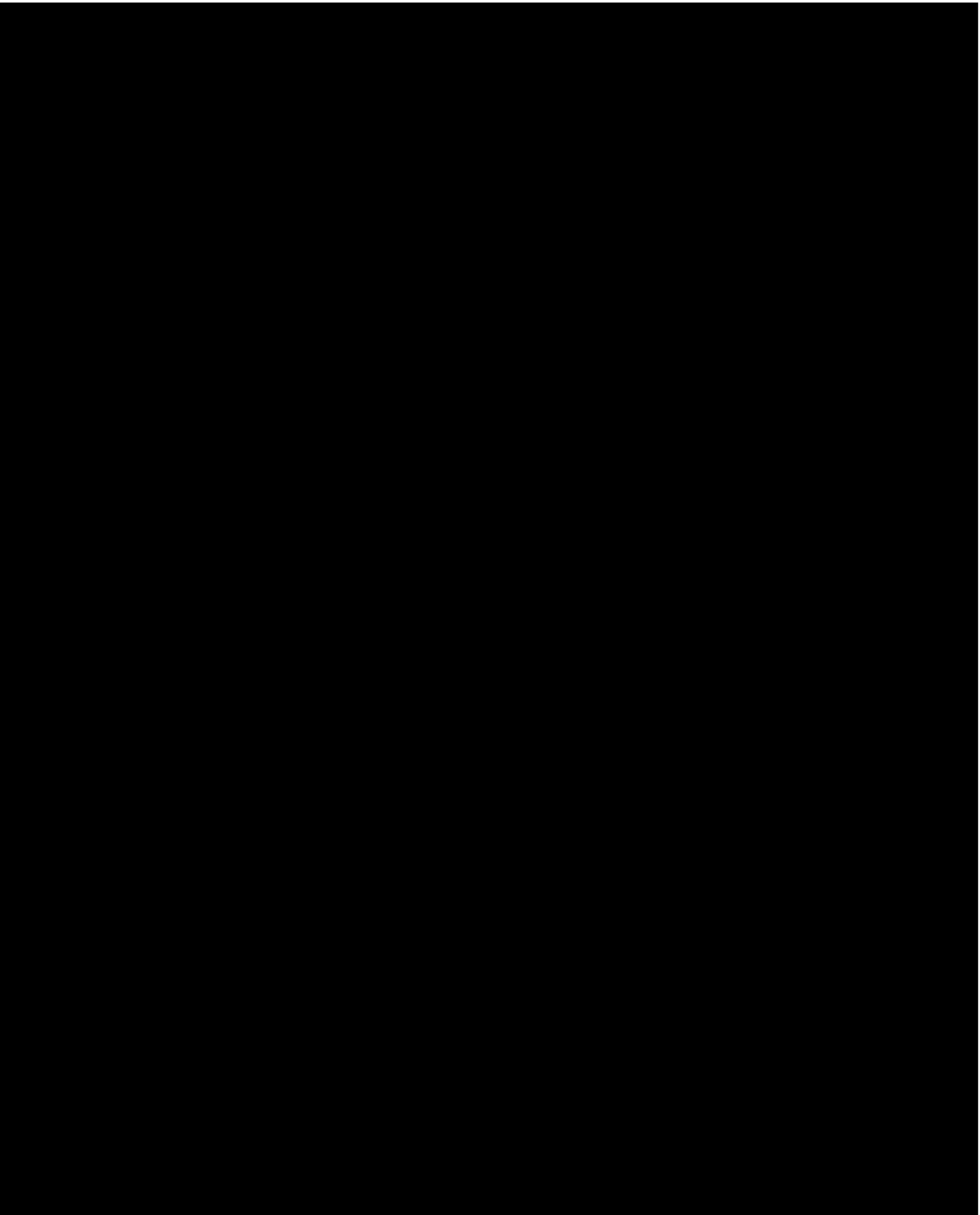
Subject: [REDACTED]

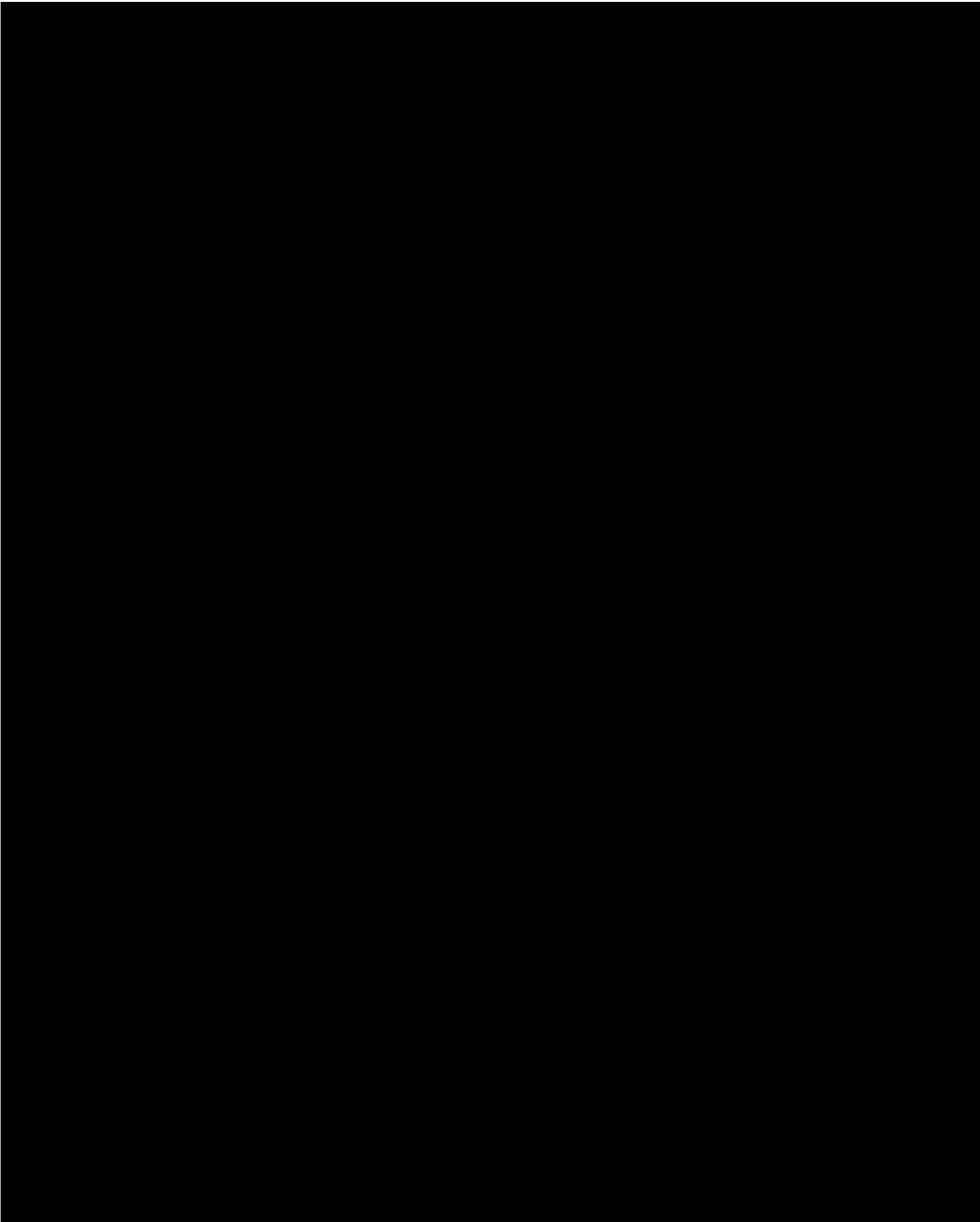
This message has been archived.


Dear Harry,











I expect that you will have further questions regarding these issues and would be pleased to answer them.

All the best,

Kent

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 9



U.S. Department of Justice

National Security Division

Washington, D.C. 20530

May 14, 2015

Kent Bressie, Esq.
Harris, Wiltshire & Grannis
1919 M Street, NW
Suite 800
Washington, D.C. 20036

Re: Application of China Mobile International (USA) Inc. for International Section 214 Authority, FCC File No. ITC-214-20110901-00289

Dear Mr. Bressie,

This letter responds to your November 21, 2014, offer to share with the Executive Branch possible mitigation measures relating to China Mobile International (USA) Inc.'s ("CMIUSA") pending application with the Federal Communications Commission ("FCC") for an authorization under Section 214 of the Communications Act of 1934, as amended ("Communications Act"), 47 U.S.C. § 214, and your November 25, 2014, request for additional information from the U.S. Department of Justice about issues or concerns regarding this application. We also received and are evaluating your January 28, 2015, message concerning your views on the workability of mitigation measures along the lines of a voting trust or proxy agreement.

As you know, the Communications Act and FCC regulations require the FCC to determine whether a grant of international Section 214 authority is consistent with the public interest, convenience, and necessity.¹ In evaluating whether granting an authorization is in the public interest, the FCC seeks the views of several Executive Branch agencies as to whether the pending application poses any "national security, law enforcement, foreign policy or trade concerns."²

Consistent with that practice, the FCC sought the views of the U.S. Department of Justice, the U.S. Department of Homeland Security, the U.S. Department of Defense, the U.S. Department of State, the U.S. Department of Commerce, the Office of Science and Technology Policy, and the Office of the United States Trade Representative as to whether CMIUSA's application for an international Section 214 authorization raises any national security, law

¹ 47 U.S.C. § 214(a); 47 C.F.R. § 63.18.

² *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market: Market Entry and Regulation of Foreign-Affiliated Entities*, FCC 97-398, 12 FCC Rcd. 23,891, 23,919 (1997) (*Foreign Participation Order*).

enforcement, foreign policy, or trade concerns. As you are likely aware, the U.S. Departments of Justice, Defense, and Homeland Security routinely coordinate, through a working group commonly referred to as "Team Telecom," in assessing particularly whether an application presents any national security or law enforcement concerns.

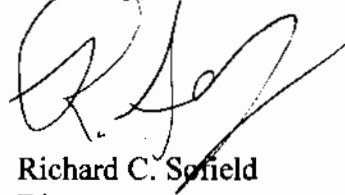
In evaluating whether a license application presents national security or law enforcement concerns, Team Telecom considers a range of factors, including but not limited to those identified below. Team Telecom is evaluating whether at least some of these factors may be implicated by CMIUSA's pending application. The factors identified below should be taken only as illustrative of the types of issues that Team Telecom considers.

- *The Applicant.* Whether the applicant has a past criminal history; whether the applicant has engaged in conduct that calls the applicant's trustworthiness into question; whether the applicant 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 or an entity controlled by or acting on behalf of a foreign government; whether the applicant's foreign ownership is from a country suspected of engaging in actions, or possessing the intention to take actions, that could impair United States national security; whether the applicant will be required, by virtue of its foreign ownership, to comply with foreign requests (e.g., requests for communications intercepts) relating to the applicant's operations within the United States, or whether the applicant is otherwise susceptible to such requests and/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 the applicant or other actors to (1) undermine the reliability and stability of the domestic communications infrastructure, (2) identify and expose national security vulnerabilities, (3) 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 United States communications infrastructure to engaged in lawful business activities, or (5) otherwise engage in activities with potential national security implications.
- *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. This consideration includes an evaluation as to the continued efficacy of confidentiality requirements that protect information about the targets of lawful surveillance, and classified sources and methods.

No factor is necessarily dispositive, and we recognize that applications can present varying degrees of risk with regard to many of these factors. To the extent an application raises identified concerns (as to the factors described above or otherwise), Team Telecom considers the relevant information and risk presented, and evaluates whether those concerns can be effectively and sufficiently mitigated through terms negotiated with the applicant relating to the scope of the authority granted or governing the applicant's conduct as it carries out its activities within the United States.

We hope that identification of these factors will assist you in developing proposed mitigation measures that you would like the U.S. Department of Justice, and Team Telecom more generally, to consider in evaluating whether possible national security or law enforcement concerns presented by your client's application for an international Section 214 authorization can be mitigated.

Sincerely,



Richard C. Seifield

Director

Foreign Investment Review Staff

CC: Shawn Cooley, DHS
CC: Harry Juricic, DOD
CC: Jonathan McHale, USTR
CC: Douglas May, DOS
CC: Evelyn Remaley, NTIA
CC: Nkechi "Payton" Iheme, OSTP

**Executive Branch Recommendation to the Federal Communications Commission to
Deny China Mobile International (USA) Inc.'s Application for an International
Section 214 Authorization**

EXHIBIT 10

12 June 2015

BY ELECTRONIC MAIL

Mr. Richard Sofield
Director, Foreign Investment Review Staff
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, N.W., Suite 6150
Washington, D.C. 20530
[REDACTED]

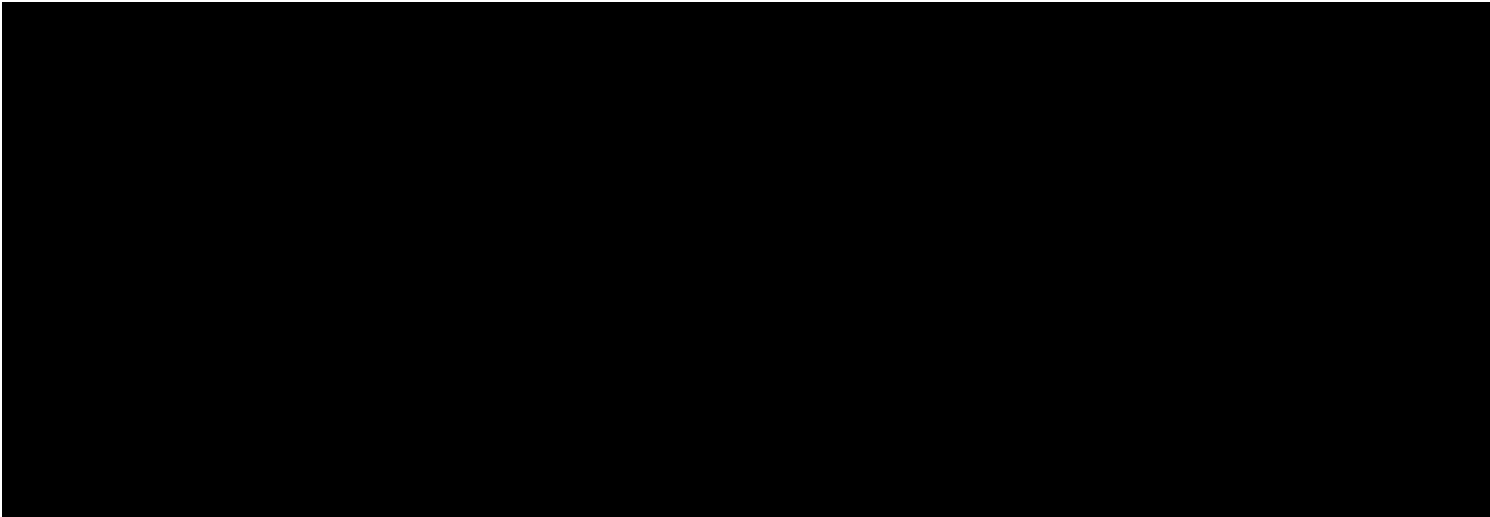
Mr. Shawn Cooley
Director – Foreign Investment Risk Management
Office of Policy
U.S. Department of Homeland Security
3801 Nebraska Avenue
Washington, D.C. 20016
[REDACTED]

Mr. Harry Juricic
Team Lead
U.S. Department of Defense
4800 Mark Center Drive
Alexandria, Virginia 22311
[REDACTED]

Re: Mitigation Proposal of China Mobile International (USA) Inc.

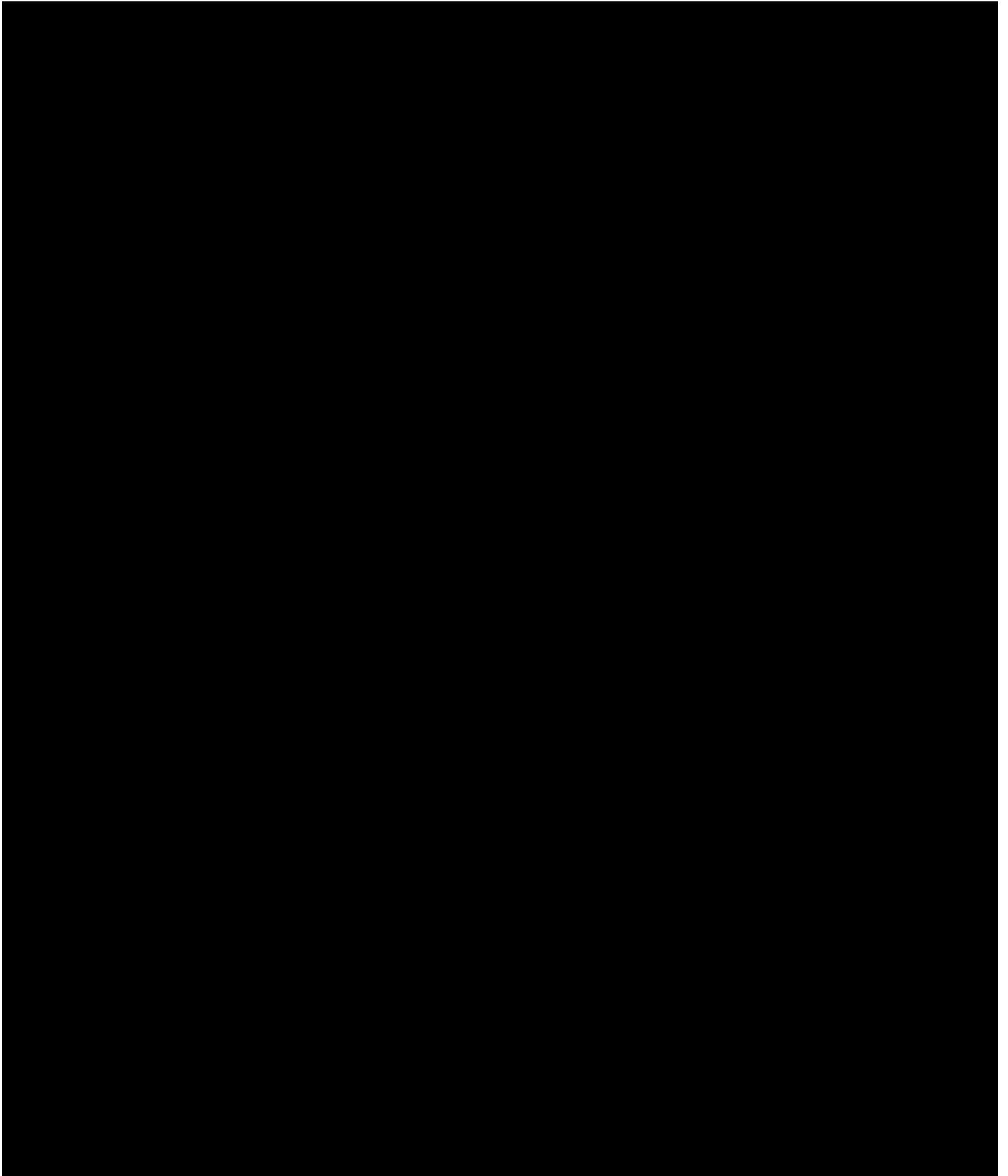
Dear Messrs. Sofield, Cooley, and Juricic:

**CONTAINS COMMERCIAL
PROPRIETARY INFORMATION
OF CMIUSA – EXEMPT FROM
DISCLOSURE UNDER
FOIA, 5 U.S.C. § 552**



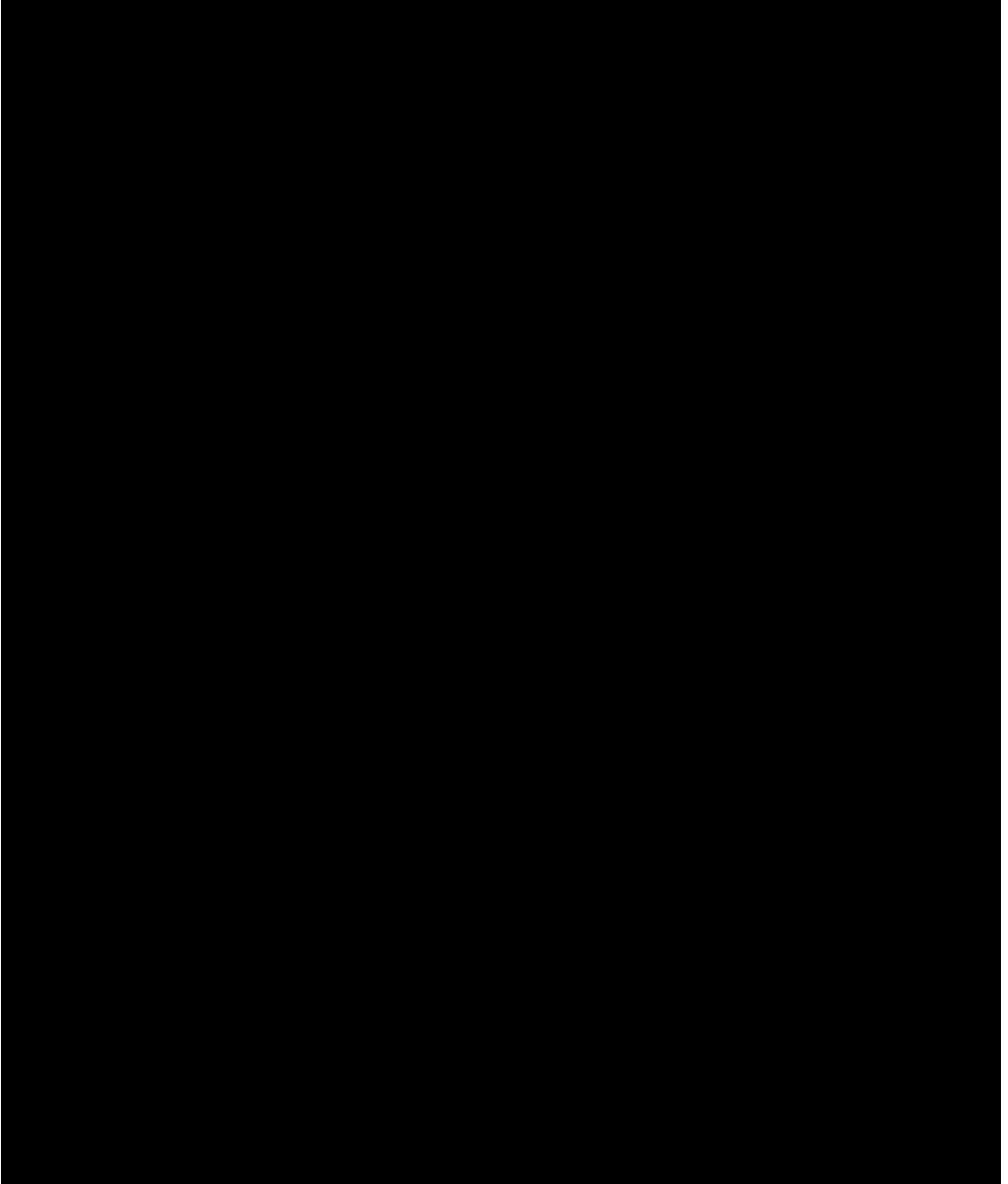
Messrs. Sofield, Cooley and Juricic
June 12, 2015
Page 2 of 6

***CONTAINS COMMERCIAL PROPRIETARY
INFORMATION OF CMIUSA – EXEMPT
FROM DISCLOSURE UNDER FOIA, 5 U.S.C. § 552***



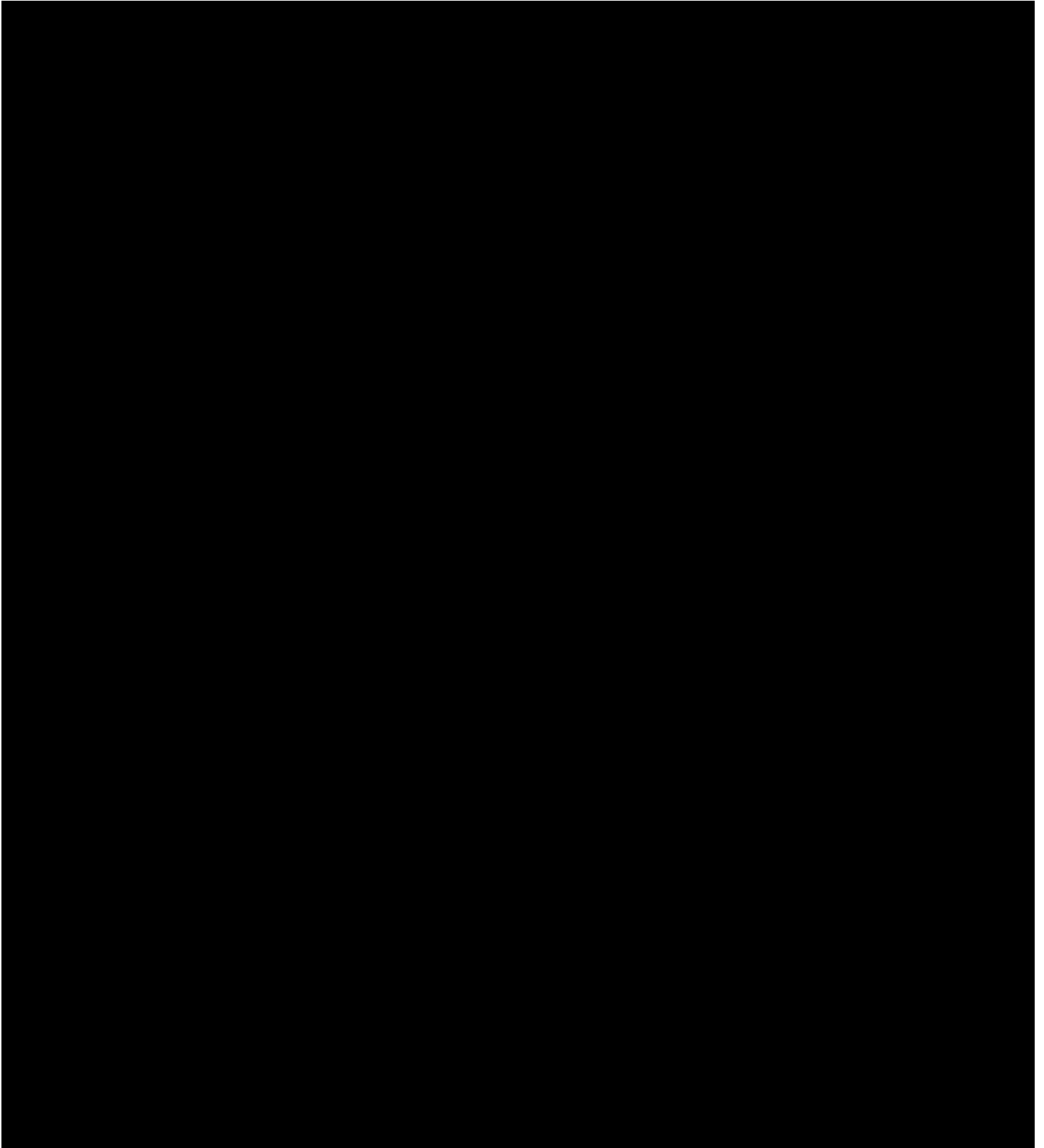
Messrs. Sofield, Cooley and Juricic
June 12, 2015
Page 3 of 6

*CONTAINS COMMERCIAL PROPRIETARY
INFORMATION OF CMIUSA – EXEMPT
FROM DISCLOSURE UNDER FOIA, 5 U.S.C. § 552*



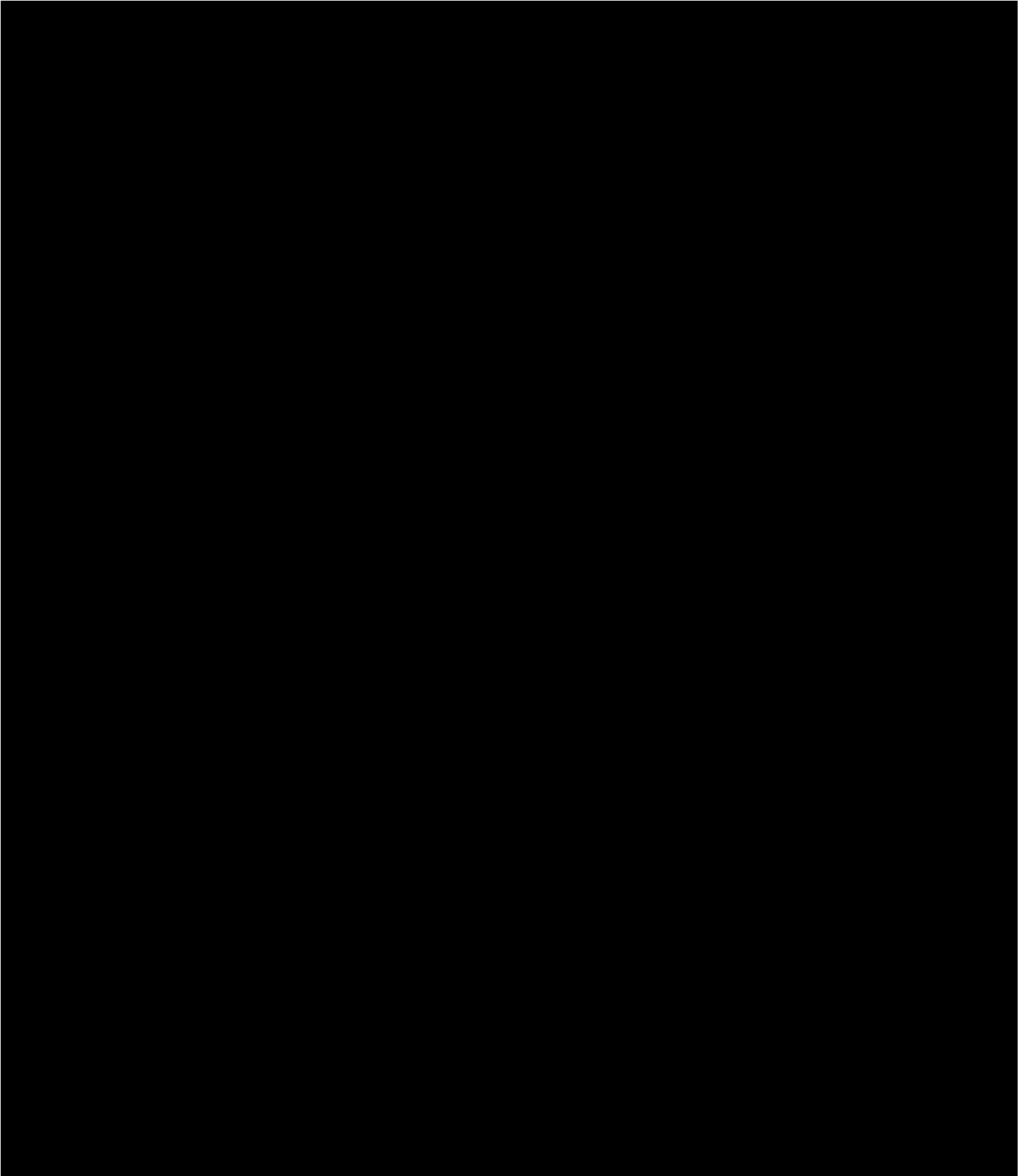
Messrs. Sofield, Cooley and Juricic
June 12, 2015
Page 4 of 6

*CONTAINS COMMERCIAL PROPRIETARY
INFORMATION OF CMIUSA – EXEMPT
FROM DISCLOSURE UNDER FOIA, 5 U.S.C. § 552*



Messrs. Sofield, Cooley and Juricic
June 12, 2015
Page 5 of 6

*CONTAINS COMMERCIAL PROPRIETARY
INFORMATION OF CMIUSA – EXEMPT
FROM DISCLOSURE UNDER FOIA, 5 U.S.C. § 552*



Messrs. Sofield, Cooley and Juricic
June 12, 2015
Page 6 of 6

*CONTAINS COMMERCIAL PROPRIETARY
INFORMATION OF CMIUSA – EXEMPT
FROM DISCLOSURE UNDER FOIA, 5 U.S.C. § 552*

Should you have any questions, please contact Kent Bressie by telephone at +1 202 [REDACTED]
[REDACTED] or by e-mail at [REDACTED].

Yours sincerely,

[REDACTED]

Kent Bressie
Patricia Paoletta
Danielle Piñeres

Counsel for China Mobile International (USA) Inc.

Attachment

cc: Team Telecom at [REDACTED] and [REDACTED]
Douglas May, U.S. Department of State
Jonathan McHale, Office of the U.S. Trade Representative
Evelyn Remaley, U.S. Department of Commerce/NTIA
Nkechi “Payton” Ihome, Office of Science and Technology Policy