STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *China Mobile International (USA) Inc. Application for Global Facilities-Based and Global Resale International Telecommunications Authority Pursuant to Section 214 of the Communications Act of 1934, as Amended*, ITC-214-200110901-00289

It's a truism to state that we live in an interconnected world. But the security environment of today is very different from what we had before the '96 Act, in which a limited number of well-established carriers interconnected with each other. Network security in those days was primarily based on simple trust, not unlike neighbors in a small town leaving their back doors open. All the players knew each other so there wasn't much risk of anyone acting maliciously.

As communications technology has evolved and new parties have entered the network, the telecom "neighborhood" has become larger and more dangerous. While the great majority of newer network participants uphold the high security standards followed by the original small group of "trusted" entities, that low security trust-based environment has become more nostalgic than practical.[1] Numerous opportunistic bad actors now have ready access to network credentials that were once limited to trusted entities. As the Executive Branch agencies state in their Recommendation regarding the application at issue here:

> 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 the ability to target, alter, block, and re-route traffic.[2]

Given our growing reliance on communications networks to support our critical infrastructure, transportation, health care and financial sector, the need for strong Commission action to address these security vulnerabilities has never been greater. Our authority is clear, beginning with Congress's explanation in Section 1 of the Communications Act of 1934 that it created the FCC both "for the purpose of the national defense" and "for the purpose of promoting safety of life and property."[3] While some have suggested that Section 1 is merely a "policy statement," the Commission has long relied upon it as informing the public interest analyses performed in numerous circumstances under both Democratic and Republican leadership, including in Section 214 proceedings like the one before us today, in our consideration of proposed transfers of broadcast and wireless licenses,[4] and in the *Supply Chain NPRM* adopted by this Commission last year.[5]

---

[1] *See* Letter from Timothy P. McKone, Executive Vice President, Federal Relations, AT&T to Senator Ron Wyden dated Oct. 13, 2017 at 1 ("At its inception, in the 1970s roughly 10 trusted carriers worldwide had access to the SS7 network. With the explosion of competition, international calling and roaming, hundreds of carriers now have access to SS7, many of them in unstable or unfriendly nations where credentials can be compromised - and, as you note, even sold on the open market for a fee. AT&T has therefore hardened and tuned our defenses to account for these developments given that the trust model is no longer fully reliable."), *available at* https://www.wyden.senate.gov/imo/media/doc/ATT%20SS7%20Response.pdf.

[2] Executive Branch Recommendation at 10.

[3] 47 U.S.C. § 151.

[4] *See Market Entry and Regulation of Foreign-Affiliated Entities*, Report and Order, 11 FCC Rcd 3873 para. 222 (1995); 47 U.S.C. § 310(d)(4) (prohibiting the grant of an FCC license to an entity exceeding the foreign ownership benchmark "if the Commission finds that the public interest will be served by the refusal or revocation of such license"); *Rules and Policies on Foreign Participation in the U.S. Telecommunications Market; Market Entry and Regulation of Foreign-Affiliated Entities*, Report and Order and Order on Reconsideration, 12 FCC Rcd 23891,

(continued….)

Nor does our authority stop there. The Act expressly gives the Commission the authority to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this Act, as may be necessary in the execution of its functions," and to "make such rules and regulations . . . as may be necessary in the execution of its functions."[6] Protecting our networks from persistent and potentially catastrophic security threats is the essence of "necessary." Congress also has specifically required the Commission to ensure that both carriers and cable operators protect the confidentiality of their customers' data.[7] Such protections, by necessity, demand secure networks.[8]

I therefore will approach any matters raising national security concerns with this authority in mind. In any such proceeding, I will review the record before me and independently assess whether the proposed outcome protects the national defense and the safety of life and property. Having come from the Department of Justice, I greatly respect the expertise of the Executive Branch agencies and will carefully consider their views and any intelligence they acquire. Nevertheless, this agency must exercise its own judgment in light of our congressional responsibilities.

With that in mind, we come to China Mobile's application for international Section 214 authority. As the item states, with a Section 214 authorization, China Mobile would be able to connect to the US

(Continued from previous page)
23918-21, paras. 59-66 (1997) (finding that national security is a factor under the Commission's public interest analysis for both Section 214 authorizations and Section 310(b)(4) determinations); *Applications of Charter Communications, Inc., Time Warner Cable Inc., and Advance/Newhouse Partnership for Consent to Assign or Transfer Control of Licenses and Authorizations*, Memorandum Opinion and Order, 31 FCC Rcd 6327, 6521, para. 429 (2015) (considering applicant's cybersecurity practices as part of the Commission's public interest standard for evaluating merger applications under Section 214(a) and 310(d) of the Act).

[5] *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket 18-89, Notice of Proposed Rulemaking, FCC 18-42 para. 36 & n.63 (rel. Apr. 17, 2018) (*Supply Chain NPRM*) (relying in part on 47 U.S.C. § 201(b)'s "public interest" authority, and citing Section 1; "Indeed, Congress similarly determined that promoting the national defense is an important public interest in section 1 of the Act, which describes the development of a 'Nation-wide … wire and radio communication service, for the purpose of the national defense' as one of the reasons for establishing the Commission.").

[6] *See* 47 U.S.C. §§ 154(i), 303(r). Additionally, the Supreme Court has repeatedly affirmed that the Commission can adopt regulations that are reasonably ancillary to the effective performance of its responsibilities. *See National Cable & Telecommunications Assn. v. Brand X Internet Services*, 545 U.S. 967 (2005); *United States v. Southwestern Cable Co.* 392 U.S. 157, 181 (1968).

[7] 47 U.S.C. §§ 222, 551(c)(1); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927, 6959, para. 64 (2007) (carriers must use "every reasonable precaution" to protect customer data); *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information*, Notice of Proposed Rulemaking, 11 FCC Rcd 12513, 12525 para. 24 n.61 (1996) ("[I]n the Cable Communications Policy Act of 1984, Congress . . . sought to restrict unauthorized use of personably identifiable information [PII] by cable operators."). *See also* 47 U.S.C. § 35; Exec. Ord. No. 10530 § 5(a) (May 10, 1954) (delegating authority to the Commission to issue submarine cable landing licenses upon a determination that, among other factors, such action "will promote the security of the United States").

[8] *See Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; IP-Enabled Services*, Report and Order and Further Notice of Proposed Rulemaking, 22 FCC Rcd 6927 at para. 36 (2007) ("[W]e make clear that carriers' existing statutory obligations to protect their customers' CPNI include a requirement that carriers take reasonable steps, which may include encryption, to protect their CPNI databases from hackers and other unauthorized attempts by third parties to access CPNI.").

telecom network and gain enhanced access to our telephone lines, fiber-optic cable, cellular networks and communications satellites. If it offers the least costly path to carry traffic on a particular route, China Mobile could even end up carrying the communications of US government agencies.

In light of the national security concerns convincingly raised here by the Executive Branch agencies and China Mobile's failure to allay those concerns, I fully support this item. But we have much more work to do if we are to fulfill our statutory duty to protect our telecommunications networks.

First, as the decision acknowledges, earlier Commissions granted international 214 authority to other carriers with similar ownership structures to that of China Mobile. The Executive Branch agencies, however, underscore how the national security environment has changed since those applications were granted, and that the risks associated with granting China Mobile's application are now heightened. It is a top priority for me to address any similar concerns Executive Branch agencies may have with other carriers. My colleagues and I should work together to do this important, and statutorily required, work.

Second, as noted earlier, a little more than one year ago, the Commission proposed to prohibit the use of USF funds for the purchase of equipment or services from any company that poses a national security threat to the integrity of US telecommunications networks or the communications supply chain.[9] While the NPRM applies only prospectively and does not require the elimination of existing equipment, Congress subsequently passed the 2019 National Defense Authorization Act, which expressly prohibits agencies, including the FCC, from obligating or expending loan or grant funds to procure or obtain equipment, services or systems that use telecom equipment by specified Chinese companies under certain conditions.[10] I firmly believe that the same security concerns raised here today are presented wherever this equipment is currently in our network. We are charged to act quickly to identify potential risks, take appropriate remedial action, and ensure that we address the needs of small rural carriers that may have this equipment in their systems. Our national security demands that we act decisively.

Finally, and more broadly, I believe the Commission needs to do more to protect the security of our telecommunications networks. As I noted earlier, Congress has charged our agency with protecting the national defense and the safety of life and property. While we may share this role with our federal partners, this agency still has the responsibility and expertise to ensure that carriers comprehensively protect the security of our telecommunications networks. As the Commission's Communications, Security, Reliability and Interoperability Council (CSRIC) has noted, both legacy and new networking systems are vulnerable to exploits like location tracking, interception, denial of service attacks and account fraud or modification.

While private sector action on these issues is laudable, the Commission needs to do more than cheer from the sidelines. We know that more steps to securing our networks are needed. According to DHS, all U.S. networks are vulnerable to surveillance by exploiting flaws in the SS7 authentication and authorization system.[11] Another study reports that one in three networks is at risk of fraud attacks like the scam where someone fools the network into forwarding them your bank's texts confirming your consent

[9] *Supply Chain NPRM*.

[10] *See Wireline Competition Bureau Seeks Comment on Section 889 of John S. McCain National Defense Authorization Act for Fiscal Year 2019*, Public Notice, WC Docket 18-89 (rel. Oct. 26, 2018).

[11] Department of Homeland Security, "Study on Mobile Device Security" at 77 (April 2017) ("[DHS] believes that all U.S. carriers are vulnerable to these exploits, resulting in risks to national security , the economy, and the Federal Government's ability to reliably execute national essential functions.") *available at* https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf (last visited May 7, 2019).

to a big withdrawal.[12] In light of these circumstances, the Commission needs to answer the following questions, among others:

- How do we address the continued operation of legacy 2G and 3G networks with known cybersecurity flaws, given that these networks can be used as entry points for attacks on more current networks? Are there particular vulnerabilities to the rural and low-income consumers who use those legacy networks?
- What measures can we take to ensure that all carriers properly utilize the security measures available in state-of-the art networks?
- How do we ensure that communications networks that receive USF support or that carry federal government communications are protected against security threats?
- How do we identify and fix any security flaws with 5G networks before their widespread deployment?

As noted above, our communications networks already underpin our utilities, transportation, financial system and health care. With this comes great responsibility. As we move into a world of 5G and the Internet of Things, our network grows larger and more interconnected than ever, and real risks and the potential harm of telecom network vulnerabilities will grow exponentially.

The days when our telecom networks could be likened to a small town safely organized around neighborly trust are long gone. We're in a new neighborhood full of both threats and opportunities, and the Commission's policies need to reflect that reality. I will be a strong voice for such change.

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

[12] Positive Technologies, "Diameter Vulnerabilities Exposure Report 2018," (June 14, 2018), *available at* https://www.ptsecurity.com/ww-en/analytics/diameter-2018/ (last visited May 6, 2019).