**KEYNOTE REMARKS OF COMMISSIONER GEOFFREY STARKS**
**AT THE AMERICAN CONFERENCE INSTITUTE**
**NATIONAL FORUM ON TEAM TELECOM**
**MARCH 17, 2021**

Thank you to ACI for inviting me today. I'm excited to discuss Team Telecom and the FCC with you, and am delighted to appear at the same event as my friend and former FCC colleague, Loyaan Egal. It seems like only yesterday that we were investigating universal service fraud issues together. But a lot has changed since then. As the last year has demonstrated, our world has never been more interconnected. Events on the other side of the planet can profoundly affect our way of life in the United States. The communications sector is no exception. Our communications network once consisted of a relatively limited group of American companies that interacted primarily on the basis of trust, not unlike neighbors in a small town leaving their back doors open. As the communications marketplace has evolved with new entrants and new technologies, however, our "neighborhood" has become larger and more dangerous. While the great majority of foreign participants present no security threat, our networks face a rising tide of activity by adversary states and other bad actors intent on compromising Americans' privacy and security. Foreign investment is critical to the growth of the US communications sector. At the same time, however, regulators must ensure that any such investment does not jeopardize our national security. That's why the FCC's partnership with Team Telecom is critical to the future of our communications networks.

That partnership begins by recognizing the important role played by both groups in reviewing foreign investments in our communications sector. As a former DOJ official, I value the expertise of our law enforcement, diplomatic, trade, and national security agencies. At the same time, I have an independent responsibility as an FCC Commissioner to assess whether the public interest supports approval of a given application. Both groups must cooperate in their review of foreign investments.

Until recently, that review presented some concerns. While the Commission and Team Telecom did their best to communicate and act quickly, applicants properly complained that the process took too long and lacked transparency. Thus, I was proud to support the FCC's action last year to update our procedures. Coupled with an Executive Order clarifying the structure and procedures on the Executive Branch side of the review process, our decision will ensure that foreign investment applications receive a thorough inter-agency review that is clear and predictable, with timely feedback.

These modernization efforts are timely. In the last several years, the United States has experienced increased malicious cyber activity by foreign agents seeking to access our networks to disrupt services, misroute information, and monitor private data. Just in the last few months, we learned that an adversary state engaged in a massive hacking attack that compromised the security of thousands of organizations, including many government agencies. And earlier this month, a leading American company disclosed that another adversary state had exploited vulnerabilities in its software to access the email accounts of organizations around the world.

Our networks have never faced greater threats, and federal policymakers must work together to ensure that those networks are secure from both external and internal attacks.

On that note, my colleagues and I initiated hearings earlier today to determine whether we should revoke the US operating authority of two Chinese-owned telecom carriers and their affiliates on national security and law enforcement grounds. In doing so, we relied on recommendations from Team Telecom, which advised us that these companies are ultimately owned and/or controlled by the Chinese government and vulnerable to its exploitation. Moreover, under Chinese law, the companies must cooperate with their government's demands for network access. These companies, therefore, pose a significant risk to both our national security and law enforcement interests, and mitigation measures are unlikely to effectively address the risks in a manner that would enable their continued operation in the United States. These are only the latest in a series of FCC decisions revoking or rejecting Chinese carriers' authority to operate in the US and constitute an excellent example of how the Commission is working with Team Telecom to protect our telecom networks against foreign adversaries.

The threats don't stop at our borders. While these actions focus on removing threats within the United States, we can't neglect other important communications areas that are subject to oversight by the FCC and Team Telecom. I've previously addressed my focus on the international carriage of traffic between the United States and the rest of the world via undersea cables. These cables, which are only about the width of a garden hose, carry 99% of the world's internet traffic. And while they've been important to international communications for a long time, their growing speed and capacity has made them essential to our modern economy and national security.

The Commission reviews applications to connect the US with these undersea cables. Because these cables are so important, the Commission and Team Telecom work together to ensure that adversary countries and other hostile actors can't tamper with, block, or intercept the communications they carry. Team Telecom has recently expressed security concerns about proposals from American tech companies and Chinese telecom carriers for undersea cables connecting our countries. I share their concerns, and the need for additional attention here. Just last week, Facebook withdrew its application for a cable between Hong Kong and California. I've also urged taking a closer look at the four existing submarine cables connecting our countries, most of which are partially owned by the same Chinese companies that are the subject of our other revocation proceedings.

Let me be clear -- undersea cables connecting the US and China are critical to our shared technological and economic future. However, the FCC and Team Telecom must be confident in the security of our communications over these connections. We also must encourage the growth of competitive alternatives to Chinese-connected cables, so they don't become the least expensive option for all our communications.

With the transition to a new Administration, it's timely to consider other national security issues regarding our communications networks. For example, even as the Commission has revoked the authority of Chinese carriers to interconnect with our telecom networks, some of

those same entities operate data centers in the United States that are not subject to FCC jurisdiction. As the Department of Homeland Security has warned, these data centers leave their customers vulnerable to data theft because Chinese law requires these companies to secretly share data with the Chinese government or other entities upon request, even if that request is illegal under US law. Currently, the FCC lacks the authority to address this potential national security threat, but as part of any review of our jurisdiction over broadband services generally, the Commission should work with the new Administration and Congress to consider whether the FCC needs broader jurisdiction to tackle this emerging network security issue as well.

We also need to continue to address the problem of insecure equipment in our networks. For nearly two years, I've led the call for the removal of Huawei and ZTE equipment from our telecom networks. Telecom carriers throughout the country purchased this equipment lawfully and in good faith, but once policymakers directed its removal, those carriers deserved help with its removal and replacement. Thus, late last year, Congress appropriated nearly $2 billion to fund the replacement of this equipment. The FCC needs to complete its proceeding implementing this legislation and begin the reimbursement process so carriers can remove this equipment and replace it with secure devices.

The equipment issues aren't limited to telecom providers. According to one study, we will have more than 25 billion connected devices worldwide by 2025. Networks of IoT devices could help reduce carbon emissions and waste, increase productivity, protect public safety, and generally enhance our way of life. But many of these devices also originate overseas, including from adversary states like China. News reports as recent as last week have highlighted security issues regarding devices like web cameras, wireless routers, and WiFi extenders. The Commission should work with other policymakers and retailers to ensure that all devices connected to our networks meet NIST cybersecurity standards. Failing to do so risks harm not only to the consumers and businesses with insecure devices but to our broader networks as a whole.

None of this is unique to the United States. Countries around the world face these same challenges. As President Biden recently said, we should stand "shoulder to shoulder" with our allies and partners to address these issues. That means the FCC must continue and expand its outreach to other countries so we can coordinate our responses and maintain a unified front on national security issues.

The FCC should also consider some internal changes. I've encouraged the agency to form a national security inter-bureau task force. The Commission currently reviews national security issues on a distributed basis among its various bureaus. For example, the International Bureau works with Team Telecom on applications to enter the US telecom market, while the Public Safety and Homeland Security Bureau participates in the National Security Council's NSPM-4 process, and the Wireline Competition and Wireless Telecommunications Bureaus consider national security in license transfers and number portability matters. This distributed structure makes internal coordination challenging and risks inconsistent treatment of national security issues between different bureaus. A national security task force would ensure that the

FCC is more coordinated, deliberative, and collaborative in managing the shifting demands of an interconnected world.

The Commission also should explore staff details with the agencies that make up Team Telecom. After years of serving primarily as a supporting agency on national security issues, a bipartisan consensus appears to have formed in support of a greater role by the FCC. That requires us to increase our in-house expertise so that we can act with confidence and gain a deeper understanding and appreciation for the work of our partners.

As technology continues to evolve and our telecom "neighborhood" continues to expand, the Commission must be collaborative and proactive in preserving national security. I look forward to working with industry and our Team Telecom partners during this new Administration to develop policies that reflect the new telecom landscape. I will continue to do everything in my power to keep Americans secure now and in the future. Thank you.