STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program,* ET Docket No. 21-232; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233.

As each day seems to bring news of another cyber-attack on our government or critical infrastructure, it has never been truer to say: "network security is national security." The Commission has assumed a critical role in this fight on several fronts. To protect the integrity of our telecommunications and information technology supply chain, we first prohibited the use of Universal Service Funding to purchase or support equipment or services posing a national security threat, then strategized a reimbursement plan to cover the cost of replacing the equipment already in U.S. networks. We've initiated proceedings to deny or revoke the US-operating authority of several foreign carriers that present a similar national security threat. I've also personally raised and focused questions about how to protect the vital communications on undersea cables and the possible threat posed by foreign-owned data centers. Today's proceeding continues these efforts by proposing to bar FCC authorizations for devices from entities deemed to present a national security risk. Congress has charged us with prohibiting untrustworthy entities from operating in U.S. networks—we shouldn't authorize equipment from those same entities for use here.

Back in 2019, I called for the Commission to examine its equipment authorization authority as a possible tool for improving our network security. Since then, I've repeatedly highlighted the need to secure our supply chain, particularly with respect to devices originating overseas. I'm therefore glad that we're moving forward with these proposed rules and I look forward to the public comments. While I recognize that the issues are complex, we cannot continue to authorize, import, and use equipment from companies deemed to present a national security threat.

In particular, I want to thank my colleagues for agreeing to three of my edits to the circulated draft. As a former enforcement official, I've seen first-hand how implementation of federal policy can be much more challenging than the initial policymaking itself. My edits therefore focused on issues following adoption of any rules and addressing the broader issue of international supply chain security.

First, if you sell your equipment in the United States—the greatest free marketplace in the world—then you should also make yourself readily available to the FCC's jurisdiction should we need to ask questions or hold you accountable for any issues stemming from that equipment. The American people welcome competition for the best goods, but also expect to be protected from harm. It is only fair. The item therefore proposes to require foreign equipment authorization applicants to have a U.S. registered agent for service of process. The Commission's staff works hard to identify and prosecute the marketing and use of unlawful equipment. Without proper service of process, however, those actions have no real consequences. I'll briefly discuss two examples illustrating this point.

In 2011, the Enforcement Bureau released a Hearing Designation Order for the Shenzhen Tangreat Technology Company based on evidence that Shenzhen had misrepresented the nature of its equipment when it applied for an FCC certification. While the company had told the FCC that its device was a "text stopper" intended to prevent texting while driving, the equipment actually operated as a jamming device, blocking cell phone signals well beyond the user's vehicle. Jammers, of course, impede authorized communications, interfere with legitimate spectrum users' rights, and jeopardize public safety. The Bureau ordered Shenzen to pay a forfeiture of more than $112,000 and to show cause why the Commission shouldn't revoke its equipment authorization.

Likewise, in 2014, the Commission found that the C.T.S. Technology Company had spent over two years illegally marketing nearly 300 models of signal jamming devices to American consumers. These included devices capable of blocking wireless signals from nearly a mile away. While C.T.S.'s devices had never obtained any equipment authorizations, the Commission proposed a significant penalty because of the egregiousness of the violations, levying a $34.9 million fine against the firm.

Years later, these cases have gone nowhere. Both Shenzen and C.T.S. are Chinese companies, and because neither firm has a U.S. agent for service of process, the Commission had to attempt service for both companies in China. Despite multiple attempts that included hiring translators, following the Hague Service Convention procedures, and contracting with Chinese service providers, the Commission has yet to actually complete service on either company. As a result, Shenzen's jamming device retains its FCC authorization, although its use remains illegal. And C.T.S. has not paid one cent to the US Treasury and probably never will.

That's not right. We need to fix this. Our proposed rules could result in an unprecedented number of proceedings to revoke equipment authorizations from the covered entities. Without policy changes, any enforcement action against these companies will undoubtedly repeat our experience with C.T.S. and Shenzen. Therefore, the NPRM proposes to require future foreign-based equipment authorization applicants to include a U.S. registered agent and asks whether this requirement should apply to all existing equipment authorizations. Relatedly, we also propose that each device submitted for FCC certification include a "responsible party" within the United States charged with ensuring compliance with our rules, consistent with our practice for Suppliers' Declarations of Conformity.

Beyond all the legalese, the point is this: if your equipment harms Americans, the FCC needs to be able to find you, and hold you accountable. These changes will hopefully increase transparency, and prevent future bad actors from using their foreign status to avoid any FCC accountability.

The implementation challenges aren't just about enforcement against foreign entities. While the key players in our equipment authorization process may closely follow any FCC rule changes, these proposals will also affect devices already in the stream of commerce or the hands of end users who may be unaware of our rules. My second edit therefore added language asking how we can educate the public about any changes in our equipment authorization rules resulting from this proceeding. Effective education will increase the likelihood of compliance by retailers, consumers, and others. We also seek comment on whether our enforcement procedures can be integrated into a consumer education effort and whether transition periods for the effective date of our rules and any enforcement may increase awareness and compliance.

Third, the item now asks how retailers can aid us in protecting the integrity of the U.S. network and supply chain. As I've noted before, even with broad adoption of industry best practices, some equipment sold in the United States may lack appropriate security protections. This is particularly likely with the inexpensive equipment sold on large websites that may be most popular with small businesses and consumers. Retailers can help protect our network security by voluntarily limiting the sale of such equipment and educating consumers about the importance of security protections for all their devices.

Finally, the revised item now asks for comment about the status of international supply chain security standards and how we can encourage greater U.S. participation in these efforts. Our economy relies on supply chains that stretch all around the world. End users expect that their devices are secure, regardless of where those devices, or their parts, originate. International standards not only provide that assurance but also increase product quality, reduce costs, and ensure a common understanding that allows manufacturers and developers to create new products that benefit consumers. For example, since 1987,

the joint technical committee of the International Organization for Standardization and the International Electrotechnical Commission has developed international standards in the field of information and communications technology, including standards which increased network security.

But China has attempted to usurp international standard setting organizations to establish economic and geopolitical power rather than enshrine the best technological approach. According to a December 2020 report from the Congressionally chartered US-China Economic and Security Review Commission, "[t]he Chinese government views technical standards as a policy tool to advance its economic and geopolitical interests. It has systematically tried to expand its influence in international standards-setting organizations by installing Chinese nationals in key leadership and functionary positions and pushing standards backed by its industrial policies." That should raise all of our eyebrows. Given China's focus on undermining the security of the U.S. and other countries, allowing it to dominate supply chain security standards could not only provide its companies with an economic edge but could also result in the incorporation of vulnerabilities for exploitation on an industry-wide basis. I say again, that's not right. We need to fix this.

Industry-led international supply chain security standards are welcome, but we must have active participation in these organizations by representatives from the U.S. and other countries that share our most important values. Greater participation on security and other issues will ensure that these bodies continue to adhere to their highest goal—that final standards reflect the best engineering and security judgments, and support the best technical outcomes. I encourage companies, universities, and other organizations to support greater participation and leadership in these bodies.

This proceeding opens up another important front in the Commission's work to protect our national security. I look forward to continuing to work on these issues and thank OET and the other Bureaus and Offices for their hard work on this item.