STATEMENT OF
COMMISSIONER BRENDAN CARR

Re: *Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program*; *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, ET Docket No. 21-232, EA Docket No. 21-233, Report and Order, Order, and Further Notice of Proposed Rulemaking

Today, the FCC takes an unprecedented step to safeguard our communications networks and strengthen America's national security. Our unanimous decision represents the first time in the FCC's history that we have voted to prohibit the authorization of communications and electronic equipment based on national security considerations. And we take this action with the broad, bipartisan backing of congressional leadership.

In March of 2021, in remarks at the Center for Strategic and International Studies (CSIS), I called for the FCC to take this action as a necessary step in our ongoing efforts to address the threats posed by Communist China and other malign actors—entities that would be all too eager to exploit backdoors in our electronics systems to obtain sensitive information and exploit that access to endanger America's interests through espionage, IP theft, blackmail, foreign influence campaigns, and other nefarious activities. At the time, I noted that the FCC's then-unprecedented decision in 2020 to prohibit the use of federal universal service subsidies to purchase equipment from companies like Huawei that pose an unacceptable national security threat represented real progress towards safeguarding our networks. Indeed, many carriers that would have otherwise purchased Huawei gear ceased doing so as a result of the FCC's 2020 rules. But as I pointed out during the CSIS remarks, those FCC rules expressly allowed carriers to use private funds to purchase the exact same equipment and place it in the exact same point in their networks. I argued that it was time to close this Huawei loophole. I am thankful that we do exactly that today.

After all, once we have determined that equipment from certain manufacturers poses an unacceptable national security risk, it makes no sense to allow that exact same equipment to be purchased and inserted into our communications networks as long as federal dollars are not involved. It is the presence of this insecure gear in our networks that presents the threat—not the source of funding used to purchase it. Yet the FCC, through its equipment authorization process, had been continuing to approve for use in the U.S. literally thousands of new applications from Huawei and other bad actors. As I noted, there is virtually no piece of electronics or communications equipment that can be used in the U.S. without an approval issued by the FCC through its equipment authorization process. So I called on the FCC to use its existing authority to deny equipment authorizations to any entity that is on the Commission's Covered List—a move that would get at the problem root and branch. Today, the FCC's Covered List includes equipment from Huawei, ZTE, Hytera, Hikvision, and Dahua.

Notably, the FCC's proposal to deny equipment authorizations involving insecure equipment garnered broad and bipartisan support. Indeed, Congress enacted and President Biden signed the Secure Equipment Act into law in November 2021 directing the FCC to complete this proceeding and in doing so provided the FCC with an additional set of authorities to act.

I also want to thank my FCC colleagues for agreeing to bolster our decision today. For instance, we now decide in this Order that the FCC has the authority to revoke existing equipment authorizations. This is an important determination, and while this Order does not take the step of revoking any equipment authorizations—focusing instead on the very important action of prohibiting the approval of new applications for covered equipment consistent with language that Congress included in the Secure

Equipment Act—I am gratified that the agency has now put revocations squarely on the table. I hope that we soon exercise that authority, and I look forward to working with my colleagues on achieving that end.

Today's decision is not a final step in our work to secure America's communication networks. Far from it. I have identified a number of additional, concrete steps we should take to protect consumers. In addition, one near term action that I recommend is for the Commission to work with the national security agencies to expand the scope of equipment from Hikvision, Dahua, and Hytera—entities with deep ties to Communist China's surveillance operation—that should be included on our Covered List. This would further strengthen our equipment authorization actions and allow us to prohibit the use of Hikvision, Dahua, and Hytera equipment in an even broader set of circumstances. We must also vigilantly monitor compliance with the rules we've established today, including by ensuring that entities do not make an end run around our decision by "white labeling" covered gear—a process that involves putting a benign or front group's name on equipment that would otherwise be subject to our prohibitions. And of course, secure networks mean little if insecure applications are allowed to run, sweep up much of the same sensitive data, and send it back to Beijing. So I would encourage the Treasury Department and the FCC's sister agencies to reach a final decision in their ongoing reviews of TikTok.

In closing, I want to offer my sincere thanks and appreciation to the many people whose hard work and leadership got us here today. To start, Chairwoman Rosenworcel deserves much credit for her longstanding commitment to protecting consumers and ensuring the Commission is engaging through the appropriate channels on national security issues. Similarly, Commissioner Starks and Commissioner Simington are champions for network security and have my appreciation for our continued partnership. Additionally, the momentum and support provided by Congress has greatly helped our ability to reach our decision today. For that, Senator Rubio, Senator Markey, Republican Whip Scalise, and Congresswoman Eshoo deserve heaps of credit. And last but of course not least, many thanks to the hardworking and talented Commission staff across the Office of Engineering and Technology, the Office of Public Safety and Homeland Security Bureau, the Office of General Counsel, the Wireline Competition Bureau, the Office of Economics and Analytics, the Enforcement Bureau, the International Bureau, and the Wireless Telecommunications Bureau who worked tirelessly on today's item.