STATEMENT OF
COMMISSIONER GEOFFREY STARKS

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

In 2019, I called for the Commission to examine its equipment authorization authority as a possible tool for improving our network security. Three years later, I'm very glad to support the Commission's action in this item. By stopping equipment identified as a threat to the United States from entering our markets, we significantly decrease the risk that it can be used against us. We also lower the possibility that we'll need to rip and replace that equipment in the future. Ultimately, if it can't get authorized, it can't be deployed.

The item is a thorough effort to secure our equipment authorization process. It amends the authorization rules to close loopholes and increases our ability to enforce our rules when a violation does occur. I want to highlight three specific policy decisions that will make a big difference in mitigating risk from untrusted and insecure equipment going forward.

First, I support amending our equipment authorization program to eliminate potential loopholes whereby equipment that is listed on our List of Covered Communications Equipment and Services (Covered List)[1] could still be authorized and allowed to enter into the United States. Specifically, by closing the possibility of using the Supplier Declaration of Conformity process if an entity produces covered equipment, we shift oversight of these higher risk entities to the certification process. This will make sure that equipment receiving authorization is clearly eligible.

Second, as a former enforcement official, I strongly support strengthening enforcement of our rules by requiring that each applicant for equipment certification designate a contact located in the United States for purposes of acting as its agent for service of process, regardless of whether the applicant is a domestic or foreign entity. When I originally proposed that the Notice do just this, it was an effort to eliminate the loophole that too many bad actors had used to evade enforcement of our rules in the past.[2] No more. If you want to be authorized to sell your equipment in the United States, we must be able to enforce our rules against you if you violate them. Full stop.

Third, the Report and Order properly eliminates equipment authorization for "white labeled equipment." White labeled equipment is equipment produced by one company that is marketed or branded under another's name. Re-branding insecure equipment does nothing to change the threat profile. In fact, it can increase risk because consumers may be more trusting of one brand than they otherwise would be if they knew who actually made it. I support the decision to close this gap that could render our new equipment authorization prohibitions less effective.

Additionally, the Further Notice seeks comment on a number of important issues. It is important that we continue to develop the record on revocation of existing equipment authorizations and a potential requirement regarding a point of presence for enforcement purposes. But, I want to focus on the importance of building a record regarding how our equipment authorization should handle components made by entities identified on the Covered List.

[1] The Covered List is available on the FCC's website at https://www.fcc.gov/supplychain/coveredlist.

[2] *Protecting Against National Security Threats to the Communications Supply Chain through the Competitive Bidding Program*, EA Docket No. 21-233, Notice of Proposed Rulemaking and Notice of Inquiry, 36 FCC Rcd 10578, Statement of Commissioner Geoffrey Starks at 1 (2021).

As the record shows, components of equipment deemed to pose a threat to the United States can pose the same risk as equipment itself. This is especially the case for advanced components or electrical components—those which can process and/or retain data. When the Commission created the Reimbursement Program, it identified the risk that certain components of Huawei and ZTE equipment could pose if—after being removed from our communications networks—those components somehow made their way back into equipment deployed in telecommunications networks. We required that both the equipment—and the components that could process and/or retain data—be destroyed,[3] consistent with Congress' direction that equipment that is removed and replaced also be destroyed.[4]

So, I'm glad my colleagues agreed to my edits to add additional questions about how the Commission should consider components of equipment listed on the Covered List. I also appreciate their support of my edits to include questions about efforts elsewhere in the United States government working on similar challenges. Specifically, we should coordinate with our fellow agencies on a whole-of-government approach with regard to components. Several agencies are working on similar efforts, such as the Hardware Bill of Materials and the Software Bill of Materials.[5] We should consider coordinating and taking advantage of the work already done by those agencies, and groups such as the Information and Communications Technology Supply Chain Risk Management Task Force,[6] to inform our actions going forward.

I thank Chairwoman Rosenworcel and my fellow Commissioners for working with me to improve the item, and for their leadership in working together to protect our nation and networks from equipment deemed to pose a threat. I thank the fantastic FCC staff, especially those in the Office of Engineering and Technology, Public Safety and Homeland Security Bureau, the Office of General Counsel, the International Bureau, the Wireless Telecommunications Bureau, the Enforcement Bureau, the Wireline Competition Bureau, and the Office of Economics and Analytics for their hard work on this challenging proceeding. This item has my strong support.

[3] *Wireline Competition Bureau Announces Best Practices for Equipment Disposal and Revises FCC Form 5640 Certifications for the Secure and Trusted Communications Networks Reimbursement Program*, WC Docket No. 18-89, Public Notice, DA 21-1234, at 14064 (Sept. 30, 2021).

[4] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1603(d)(7). *See also* H.R. Rep. No. 116-352, at 14 (2019) ("Any applicant receiving reimbursement funds under the Program is required to complete the permanent removal, replacement, and disposal of covered equipment and services from their networks not later than one year after the date on which the Commission distributes funds to the applicant.").

[5] Software Bill of Materials, Cybersecurity and Infrastructure Security Agency, *available at* https://www.cisa.gov/sbom (last visited Nov. 22, 2022).

[6] ICT Supply Chain Risk Management Task Force, Cybersecurity and Infrastructure Security Agency, *available at* https://www.cisa.gov/ict-scrm-task-force (last visited Nov. 22, 2022).