STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Connect America Fund, et al.*, WC Docket Nos. 10-90, No. 14-58, 09-197, 16-271, RM-11868, Notice of Proposed Rulemaking (May 19, 2022).

The availability and affordability of broadband access nationwide is one of the highest priorities of the Commission, and personally, to me as a Commissioner. Another is ensuring that our networks are secure. This Notice of Proposed Rulemaking offers the opportunity to vote to seek comment on both, and I am proud to do so.

First, the item seeks comment on a proposal by the ACAM Broadband Coalition to expand our Alternative Connect American Model (A-CAM) plans in both scope and duration. With additional funding and an expansion of the length of time under which electing carriers would receive support, these carriers would increase deployment speeds up to 100 Mbps download, and 20 Mbps upload in some of the most challenging and expensive areas to serve in the country. If the Commission accepts this proposal, after a thorough review of the record that develops, some consumers served by A-CAM carriers could see a 4-fold, 10-fold, or even 20-fold increase in their speeds. That would be a big win. At the same time, the item appropriately seeks comment on affordability, and how to ensure those least available to afford broadband can participate in the benefits of these federally subsidized networks. Additionally, the increase in funding available could encourage other rate-of-return carriers to sign up for this Enhanced A-CAM. Moving carriers from legacy support to model-based support has been a Commission goal, and I support it.

This is a fitting time to be discussing the future of A-CAM. NTIA only days ago released its Notice of Funding Opportunity for the $42 billion dollar Broadband Equity, Access, and Deployment Program, often referred to as BEAD. It is instructive—in particular on our expectations of future build-outs. Specifically, one place where I look forward to understanding further after reviewing the record is the alignment between the short BEAD build-out window and the proposed timeframe submitted by the A-CAM providers. More holistically, our Notice appropriately seeks comment on how our A-CAM program can complement BEAD, and I look forward to reviewing the comments to see how the programs can work together.

It is critical that we look at any A-CAM expansion with an eye on BEAD, because one thing that can't happen is for either A-CAM or BEAD to overbuild or waste support. I take our role as a steward of the Universal Service Fund seriously, and we must ensure that this once-in-a-lifetime federal support is used to deliver broadband at competitive speeds in places where it has so far been lacking. The two programs, if they work together, will be able to expand broadband to benefit previously unserved and underserved communities, especially, in low-income communities, communities of black and brown majorities that have so often been overlooked, and in rural communities desperate for access to service to participate in our connected society. The stakes are high: for our part here at the FCC, we're spending an enormous amount of ratepayer money, and the communities waiting for broadband infrastructure have been waiting too long.

Second, networks that are subsidized and built with federal funds must be secure. This is evident in the constant barrage of attacks on American networks from hostile state and non-state actors. To mention a few, in March 2022, hackers linked to the Chinese government penetrated the networks belonging to government agencies of at least six different U.S. states in an espionage operation.[1] Kremlin-linked threat actors hacked into numerous defense contractors between January 2020 and

[1] Center for Strategic and International Studies, *Significant Cyber Incidents*, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (CSIS Significant Cyber Incidents).

February 2022,[2] and ransomware continues to be an ongoing problem for critical infrastructure[3] and local governments.[4] Further, while not domestic, we have all seen the constant attacks against Ukrainian networks.[5]

So I'm proud to announce that my colleagues have agreed with my ask to include, for the first time, a request for comment on whether we should require A-CAM carriers and carriers receiving high cost support to have baseline cybersecurity and supply chain risk management plans. The Notice now seeks comment on whether these plans should spell out specific security and privacy controls, in the case of cybersecurity, and supply chain risk management controls being implemented. It also asks whether the plans should reflect the resources of our expert government agencies, such as the National Institute of Standards and Technology. These cybersecurity and supply chain risk management plans, if ultimately included as a requirement in future A-CAM and other high cost support programs, will ensure a baseline of support to protect American communications networks and United States citizens from threats from adversaries and bad actors. I note, again, that this proposal is aligned with a similar requirement in the BEAD program, which makes sense, because as we seek comment on how the two programs can support each other, it is imperative for us to ensure that FCC-funded networks are as equally secure as those from other portions of the federal government. These A-CAM networks must stand shoulder to shoulder with the BEAD build-out.

I fully expect that going forward, as the Commission reviews and supports broadband build-out such as the high cost program, these types of cybersecurity and supply chain risk management baseline requirements will be fundamental to our consideration. While this Notice seeks comment on the ACAM Broadband Coalition's proposal, it also seeks comment on how to improve administration of the high cost program, and whether baseline cybersecurity and supply chain risk management plans should be required for carriers receiving high cost support. It is critical that federally subsidized networks are secure if consumers are to have the confidence to use them to their fullest.

I'm excited for the Commission to take this initial step, and I thank the Chairwoman for agreeing to my additions and for her leadership in protecting our networks more generally, and for the support of my fellow Commissioners as well. I also thank the Commission's staff that has worked tirelessly on these broadband programs. The item has my full support.

---

[2] *Id.*

[3] Department of Energy, Office of Cybersecurity, Energy Security, and Nuclear Response, *Colonial Pipeline Cyber Incident*, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident.

[4] Ionut Arghire, FBI Warns of Ransomware Attacks Targeting Local Governments, Securityweek.com, https://www.securityweek.com/fbi-warns-ransomware-attacks-targeting-local-governments (Apr. 1, 2022).

[5] *See, e.g.*, CSIS Significant Cyber Incidents.