STATEMENT OF COMMISSIONER GEOFFREY STARKS

Re: *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Report and Order and Further Notice of Proposed Rulemaking (March 14, 2024).

Everywhere we look, the term "connected" is attached to products that formerly lacked it. Products that exist in all of our homes—lightbulbs, thermostats, locks, doorbells, smoke alarms, and even your toaster and refrigerator—now often come standard with wireless capability and the ability to access and control a device through the Internet. This innovation, though, is not costless. Far too many Internet of Things (IoT) products include lackluster security features, if any at all. This is a risk to all of us because insecure and cheap IoT products can threaten our security, our privacy, and more. They can allow remote access to our homes, allow bad actors to monitor our comings and goings remotely, lead to data theft, or, if enough insecure IoT products are combined to form a network, create botnets that can wreak havoc throughout the Internet through denial of service attacks.

We've known about these risks a long time, and today's Order is the culmination of years of work by the Biden Administration, the National Institute of Standards and Technology (NIST), government agencies, and private stakeholders. With the proliferation of connected products available it is challenging, even for the most informed consumer, to confidently identify the cybersecurity capabilities of an IoT device. But help is on the way. Once the Cyber Trust Mark is up and running, consumers will only need to look at the product packaging to determine whether the product meets the standards keyed to NIST's *Profile of the IoT Core Baseline for Consumer Products* (NISTIR 8425). By simply scanning a QR code on the product, consumers can learn more about specific security features, including, for example, the minimum support period for the product and instructions on how to change the default password. Consumers can purchase with confidence knowing that the product, including components such as the backend and mobile app necessary to use the IoT product, meet baseline standards.

This Cyber Trust Mark is ready to meet the moment. Stories abound about the prevalence of insecure IoT devices. Just last week, following yet another report of cheap, insecure IoT devices made from China flooding markets in the United States, I sent letters to five leading retailers to learn more about the sale, and promotion, of easily hackable video doorbells that lack even basic security measures.[1] I also asked about their plans to incorporate the Cyber Trust Mark into their marketplaces to help consumers identify IoT products that meet the Mark's level of security. I look forward to reviewing their responses, and working together to stop risky and insecure products from entering the commerce stream.

I strongly support the Order we adopt today, and believe the item strikes an appropriate balance between a voluntary program that entices manufacturers and retailers to participate with teeth to protect consumers. I particularly would like to thank Chairwoman Rosenworcel for her leadership and for supporting my ideas to properly scope the Cyber Trust Mark. As I signaled when we considered the *Notice*, I believed then that the proper scope for the Cyber Trust Mark needed to be "products," not "devices." The Order we adopt today adhered to that policy cut, and I believe gets it right that the best frame for the Cyber Trust Mark is IoT products. This is consistent with NISTIR 8425, as well as consumer expectations, and will ensure that the Cyber

[1] *FCC Commissioner Geoffrey Starks Calls on Online Marketplaces to Stop the Sale of Insecure and Unauthorized IoT Devices*, Release, Mar. 8, 2024, https://docs.fcc.gov/public/attachments/DOC-401038A1.pdf.

Trust Mark is both successful domestically and can achieve mutual recognition internationally with other cyber labeling programs that focus on IoT products.

Second, I maintain that it is imperative that we do not place our stamp of approval on devices from products that any branch of the United States government and our allies have identified as part of a national security review. I'm very happy that the Order keeps that policy as well, excluding from the Cyber Trust Mark equipment produced by any entity on our Covered List, the Department of Commerce's Entity List, and the Department of Defense's List of Chinese Military Companies. I'm also very happy that this prohibition applies to Cybersecurity Label Administrators and CyberLABs participating in the Cyber Trust Mark.

Third, I thank the Chairwoman for agreeing to language in the Order to make clear that the Lead Administrator should ensure that the Cyber Trust Mark standards are dynamic and updated when NIST adopts additional recommendations for routers, cloud, and other aspects of the IoT ecosystem that it is currently considering. Making it clear that our standards are not stagnant will ensure that consumers are protected as technology and manufacturers innovate.

Much work remains before we see the first Cyber Trust Mark label on a product's packaging, but with today's vote we are closer than ever. Once the Cyber Trust Mark is available, I look forward to the innovation that I expect will occur from consumers and the federal government purchasing and deploying IoT products with confidence knowing that those products meet the core baseline for IoT cybersecurity. I thank staff for their great work on this item. I strongly approve.