STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

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

Internet of Things devices are all around us. They are multiplying—fast. If you buy a television, a thermostat, a home security camera, or a fitness tracker today the odds are it is connected the internet. These smart devices make our lives easier and more convenient. They mean we can watch what we want, turn down the heat when we are away, check who is at the front door when we are not home, and keep tabs on our health at all times. It is extraordinary.

Still, the device that I think of most when I think about this new world of the Internet of Things—and maybe it is because I am a Mom—is a baby monitor. My goodness, you want that to be safe. You want to know when you bring that monitor into your house to watch your newborn, that connection is secure and not going to invite any malware or malicious activity into your home. I think parents everywhere feel this way.

So what do we do about it? What can we do to make sure that the conveniences billions of these devices offer do not come with the downside of increased security risk? How do we make sure the everyday connections in our homes are safe?

These are the right questions to ask. Because this increase in connection brings more that convenience. It brings cyber vulnerabilities. After all, every device connected to the internet is a point of entry for the kind of attacks that steal our personal data and can compromise our safety.

That is why today the Federal Communications Commission establishes the first-ever voluntary cybersecurity labeling program for connected smart devices in the United States. The label is called the U.S. Cyber Trust Mark. When it is displayed, it will mean that the device has been certified to meet cybersecurity standards. The label will include a QR code linking to a product registry that will provide consumer-friendly information. Just like the "Energy Star" logo helps us know which devices are energy efficient, the Cyber Trust Mark will help us make informed choices about the security and privacy of Internet of Things products we bring into our homes and businesses.

We are building the Cyber Trust Mark program on the well-known cybersecurity criteria developed by the National Institute of Standards and Technology. We are also building this effort on the existing model we have at this agency for authorization of devices using radio frequency. So we have both a framework for standards and a framework for execution. To get it done, we will need expert partners. We will select third-party administrators, including a Lead Administrator, through a rigorous selection process that will work with us on the day-to-day details of the program. The administrators selected will be responsible for receiving and reviewing applications from manufacturers to use the Cyber Trust Mark.

From the start, we are building national security into the program. No entity or communications equipment from what is known as the "Covered List" is eligible for a label. And in the a further rulemaking we ask questions if manufacturers should be required to disclose if firmware or software in the product was developed in a country that is a foreign adversary.

Our expectation is that over time more companies will use the Cyber Trust Mark—and more consumers will demand it. This has the power to become the worldwide standard for secure Internet of Things devices. To get to this point, we know we need to work with our federal partners, manufacturers, retailers, and cybersecurity groups. We are ready to do just that.

This is no small task. But it's worth it. Because the future of smart devices is big and the opportunity for the United States to lead the world with a global signal of trust is even greater. I appreciate working with my colleagues on establishing this program and look forward to seeing the Cyber Trust Mark in the marketplace.

I want to thank the staff responsible for this effort including Steven Carpenter, Rochelle Cohen, Josh Gehret, Ahmed Lahjouji, Zoe Li, Nicole McGinnis, Drew Morin, Renee Roland, Tara Shostek, and James Zigouris from the Public Safety and Homeland Security Bureau; Brian Butler, Dana Shaffer, Paul Murray, Jamison Prime, George Tannahill, and Krista Witanowski from the Office of Engineering and Technology; Edward Carlson, Jared Carlson, and Brandon Moss from the Office of International Affairs; Regina Brown and Sarah Stone from the Office of the Managing Director; Hunter Deeley, Matthew Gibson, Jason Koslofsky, Shannon Lipp, Jeremy Marcus, Ryan McDonald, Elizabeth Mumaw, and Victoria Randazzo from the Enforcement Bureau; Joy Ragsdale and Chana Wilkerson from the Office of Communications Business Opportunities; Eugene Kiselev, Mack Wachala, and Aleks Yankelevich from the Office of Economics and Analytics; and Erika Olsen, Larry Atlas, Andrea Kelly, Doug Klein, Marcus Maher, Karen Schroeder, Jeff Steinberg, and Chin Yoo from the Office of General Counsel.