STATEMENT OF
CHAIRWOMAN JESSICA ROSENWORCEL

Re: *Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Notice of Proposed Rulemaking (August 8, 2023)

There are so many new devices—from smart televisions and thermostats to home security cameras, baby monitors, and fitness trackers—that are connected to the internet. In fact, right now there are estimates that there are 17 billion smart devices in the world, and that number is expected to increase to 25 billion by the end of the decade. These technologies provide all kinds of benefits because they can make our lives easier and more efficient. They allow us to do things like check who is at the front door when we are away, keep tabs on our health, and automatically adjust the thermostat, so we save on our energy bills.

However, this increased interconnection brings more than just convenience. It brings increased security risk. After all, every device connected to the internet is a point of entry for the kind of cyberattacks that can take our personal data and compromise our safety. That is true for the biggest connections to the largest businesses and the smallest connections to the devices in our homes.

I believe it doesn't have to be this way. That's because we can do more to make internet of things devices secure and help consumers make good choices about what they bring into their homes and businesses.

This is exactly what we propose to do so with this rulemaking. We propose to put in place the first-ever voluntary cybersecurity labeling program for connected smart devices. We are calling it the U.S. Cyber Trust Mark. And just like the "Energy Star" logo helps consumers know what devices are energy efficient, the Cyber Trust Mark will help consumers make more informed purchasing decisions about device privacy and security. So when you need a baby monitor or new home appliance, you will be able to look for the Cyber Trust Mark and shop with greater confidence. What's more, because we know devices and services are not static, we are proposing that along with the mark we will have a QR code that provides up-to-date information on that device.

This proposal builds on good work already done by government and industry because we will rely on the NIST-recommended criteria for cybersecurity to set the Cyber Trust Mark program up. That means we will use criteria device manufacturers already know, and, when they choose to meet these standards, they will be able to showcase privacy and security in the marketplace by displaying this mark. Over time, we hope more companies will use it—and more consumers will demand it.

With this notice we seek input on how best to establish this voluntary labeling program, the scope of eligible devices, the mechanics of managing this program, how to further develop standards that could apply to different kinds of devices, how to demonstrate compliance with those standards, and how best to educate consumers.

That is not a 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 the interest my colleagues have expressed in this effort, look forward to the record that follows, and in the future seeing the Cyber Trust Mark in the marketplace.