STATEMENT OF
COMMISSIONER NATHAN SIMINGTON

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

I'm thrilled that we are enacting this order today. I'm not exaggerating when I say that it has the potential to be the beginning of a new era for American cybersecurity policy.

It is long established law in this country that if your car explodes in a minor accident, if a table saw comes loose and maims you, or if your lightbulb overheats and causes a fire, you can take the negligent product manufacturer to court and recover your damages. This gives manufacturers a strong incentive to design safe products. But if an attacker hacks your smart home device, like an Alexa, and steals your financial information or listens in on your private conversations, you have little to no recourse against the manufacturer, even if the attack was only possible due to its negligent cybersecurity practices. This is because device manufacturers and software developers routinely disclaim all liability and warranties against such failures and tort law provides few protections in the absence of physical injury to persons or property.

I've become increasingly alarmed at this gap in our legal system, and in December of 2022, I first argued for using our authority under Title III to address negligent cybersecurity practices by wireless device manufacturers, on the theory that hacked devices could be used to cause harmful interference. Today, we use exactly that theory to institute this program, a massive first step in bringing legal accountability to the device industry. I worked hard to make sure that the program will set a high bar for the security of wireless devices. If manufacturers want to be eligible for the US Cyber Trust Mark, they will have to declare that they have taken every reasonable measure to create a secure device.[1] They will have to commit to a support period up front, and during that support period, they will have to diligently identify critical vulnerabilities in their products and promptly release updates correcting them. Crucially, they will be prohibited from disclaiming these promises to the consumer. As a result, these promises will be enforceable not only by the FCC itself, but also by the courts of every state under product warranty and contract law.

Importantly, this program is optional. The IoT market is incredibly dynamic and innovative—and young. The risk of inadvertently stifling it with overregulation is real. So instead of imposing mandatory rules, we are setting a high bar for products to earn the right to use the US Cyber Trust Mark and hoping that consumers and businesses begin to value that mark because it means that the manufacturer is confident enough about the security of their product, and their processes for patching security flaws, that they are willing to stand behind the product legally. Over time, I hope that consumers and businesses, and their insurers, begin to insist that the products they buy bear this mark.

More work remains to be done. I'm happy that the Chairwoman's office agreed to include a further notice of proposed rulemaking on the issue of how to handle devices that run

[1] In recognition of the fact that a device's security might reasonably depend on the actions of its owner and users, the order uses the term "securable."

software developed in hostile countries, that will receive updates deployed from or that can be controlled by servers in such countries, or that will store user data in those countries. Such devices are at high risk of being weaponized by hostile powers like China. It is incredibly easy to hide a backdoor in an IoT device, and almost impossible to detect it, as a good backdoor is indistinguishable from an accidental coding mistake. The House of Representatives voted to ban one trojan horse yesterday, TikTok, and here at the FCC we need to make sure that consumers and businesses are aware if they might be buying another one.

We will also need to figure out how to expand this program to computers, smartphones, routers, and non-consumer devices generally. I hope that as we do so, we focus less on bureaucratic processes and checkbox compliance exercises and more on simply requiring the manufacturers and software developers behind those products to put their skin in the game and stop hiding behind broad disclaimers of warranties and liability if they want their products to bear the US Cyber Trust Mark.

Thank you to the Chairwoman's office, other Commissioners, and staff for working with me on getting this item right.