STATEMENT OF COMMISSIONER NATHAN SIMINGTON

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

Cybersecurity vulnerabilities are inevitable. Even the best engineers, supported by sophisticated organizations and applying the best software development methodologies, cannot hope to eradicate every security flaw lurking in a modern software-powered device. A single one of these vulnerabilities can be enough to render access controls and other security mechanisms useless, allowing even amateur attackers to bypass them and gain illicit access to sensitive information and controls. Because any device is liable to be rendered insecure at any time by a newly discovered flaw, a responsible manufacturer should undertake to search for and patch vulnerabilities as quickly as possible. Otherwise, it might as well be putting ticking time-bombs into the homes and businesses of every one of its customers across the country.

Unfortunately, many device companies have fallen short. It often takes months for a fix to a serious vulnerability to make its way to end user devices, if the manufacturer bothers to release an update at all, and if the device was designed to be updateable in the first place. Manufacturers frequently pull the plug on support for a device well before consumers have stopped using it. The length of security support periods—the time period during which users can count on receiving timely security updates—is usually not communicated at the time of sale, and sometimes the end of support is not even announced, leaving even the most informed users unsure whether their devices are still safe to use. And many devices require manual installation of security updates, something very few consumers will ever do.

This is no mere academic concern. Attacks on unpatched devices are becoming more frequent and more dangerous. A recent FBI advisory warned of increasing cyberattacks against unpatched medical devices.[1] Unpatched industrial control systems threaten the availability of critical infrastructure.[2] The Mirai botnet, which at its peak consisted of over 600,000 compromised devices performing large-scale cyberattacks in unison, grew by scanning the internet for devices with unpatched vulnerabilities like IP cameras and routers and taking control of them.[3] And we have not yet seen the worst. An attacker could use unpatched vulnerabilities to take control of large numbers of mobile phones, turn their radios into signal jammers, and take down mobile networks.[4] Botnets of commandeered high wattage devices like air conditioners, water heaters, and ovens could be used to disrupt the power grid and even cause large-scale blackouts.[5] And attacks on cyberphysical systems like automated cars, or on medical devices, can directly cause widespread property destruction, human injury, and death.

The early days of the connected device industry are behind us, and the laissez-faire attitude that came with rapid innovation now threatens to thwart the industry's progress into more serious domains where the stakes are higher. As we entrust technology with greater responsibility for our money, privacy, personal safety, and public order, we need to have greater confidence in its security. Otherwise,

[1] https://www.ic3.gov/Media/News/2022/220912.pdf

[2] https://www.darkreading.com/vulnerabilities-threats/cisa-warns-unpatched-vulnerabilities-ics-critical-infrastructure; https://www.cisa.gov/news-events/alerts/2023/03/21/cisa-releases-seven-industrial-control-systems-advisories; https://www.darkreading.com/ics-ot/unpatched-iot-ot-devices-pile-up-ics-cyberattacks

[3] https://blog.cloudflare.com/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/; https://www.scmagazine.com/news/unpatched-apache-tomcat-servers-spread-mirai-botnet-malware; https://www.theregister.com/2023/05/02/cisa_exploited_flaws_oracle_apache/

[4] https://www.cise.ufl.edu/~traynor/papers/ccs09a.pdf

[5] https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf

increasingly damaging cyberattacks will undermine faith in automated systems and prevent us from realizing the full gains in productivity and quality of life that the technological revolution promises.

I am only able to support this initiative because it includes my proposal that the cybersecurity labels disclose the time period during which a device's manufacturer commits to diligently issue security updates. A stamp of approval from the United States government for the security of your device should reflect the genuine confidence of the American people. You cannot possibly qualify for such an endorsement if you refuse to provide even this bare minimum of transparency. If you want this label on your product, you must earn it by taking responsibility for the security of your product, not just while you initially develop it, but for its entire lifespan. Requiring any less would make the United States government complicit in reckless conduct that endangers the safety and security of every American. I want to thank the Chairwoman and the other Commissioners for supporting my request that we include this provision.

I suspect that some manufacturers will choose to not pursue a label rather than commit themselves to doing the right thing. The United States government should be proud to deny such companies a label. Let the absence of a label serve as a warning: this device is not safe.