STATEMENT OF
COMMISSIONER GEOFFREY STARKS

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

Nearly 40 years ago David Nicols had a problem. As a graduate student enrolled in Carnegie Mellon University's computer science department he needed a caffeine hit, but it was a hike to reach the soda machine in his building, and it frequently ran out. He wanted a tool to stop the trend of returning from his long walks empty-handed. So, he did what any enterprising computer scientist would do—he solved the problem using technology. He and some friends created an application that monitored the soda machine's reserves and connected it to ARPANET, the Internet's forerunner, so they could remotely view the soda availability and temperature. In doing so, we now know, they actually created the very first Internet of Things (IoT) device.[1] It was a success, to say the least! Another student followed suit, focusing on the nearby M&M machine, and it was off to the races.[2]

From those humble beginnings, it's now hard to imagine an electronic device that isn't connected. One manufacturer estimates that there are more than 20 billion IoT devices in active use around the world,[3] and it is estimated that spending on IoT surpassed $1 trillion dollars in 2022, and will be even higher this year.[4] On this front, I saw continued momentum firsthand when I visited this year's Consumer Electronics Show earlier this year.

The proliferation of IoT devices has, of course, led to many benefits in society. At the same time, their use has elevated the United States' risk profile due to their prevalence in our networks and physical world. Without the right level of security, they constitute an attack plane that can introduce vulnerabilities, both individually or as part of a network of IoT devices working together, sometimes referred to as botnets. This threat occurs due to the fact that historically, many IoT devices were created and deployed without necessary baseline cybersecurity protections, which bad actors can exploit.[5] Unprotected IoT devices and devices with simple or no security such as easily guessable default passwords are susceptible to malware[6] and hacking, and can be used to create botnets that can wreak havoc on our networks. These unsecure IoT devices when used maliciously can block access to the Internet and websites, waste network resources, and cause harm to people, businesses, and government alike.

---

[1] The Carnegie Melon University Computer Science Coke Machine, *The 'Only' Coke Machine on the Internet*, Carnegie Melon, *available at* https://www.cs.cmu.edu/~coke/history_long.txt.

[2] Jordan Teicher, *The Little Known Story of the First IoT Device*, IBM.com, Feb. 7, 2018, *available at* https://www.ibm.com/blog/little-known-story-first-iot-device/ (The Little Known Story of the First IoT Device).

[3] Nokia Threat Intelligence Report Finds Malicious IoT Botnet Activity Has Sharply Increased, Press Release, Nokia.com, June 7, 2023, *available at* https://www.nokia.com/about-us/news/releases/2023/06/07/nokia-threat-intelligence-report-finds-malicious-iot-botnet-activity-has-sharply-increased/.

[4] IDC Report: IoT Spending to Reach More than $1 Tillion by 2022, Finley Research (Last visited Aug. 8, 2023), *available at* https://finleyusa.com/idc-report-iot-spending-to-reach-more-than-1-trillion-by-2022/#:~:text=Telecom%2C%20Broadband-,IDC%20Report%3A%20IoT%20Spending%20to%20Reach%20More%20than%20%241%20Trillion,%24646%20billion%20spent%20last%20year.

[5] Alert, Secure New Internet-Connected Devices, Cybersecurity and Infrastructure Security Agency, Dec. 31, 2019, *available at* https://www.cisa.gov/news-events/alerts/2019/12/31/secure-new-internet-connected-devices.

[6] 2022 Sonicwall Cyber Threat Report, Mid-Year Update, Sonicwall (Last visited Aug. 8, 2023), *available at* https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2022-cyber-threat-report.pdf (finding a 77% increase in malware attacks for IoT/Connected Devices in the first half of 2022).

Recognizing the problem, the United States government has taken steps to mitigate the risks and improve security. Beginning in 2018, the Department of Commerce's *Botnet Report* identified actions to protect devices and networks including the idea of a labeling program.[7] President Biden drew on that approach when releasing his *Executive Order on Improving the Nation's Cybersecurity*, EO 14028, requiring an IoT labeling pilot.[8] President Biden's *National Cybersecurity Strategy* went further and included driving the development of secure IoT devices as a strategic objective.[9]

That leads us to this proposal, which is the cumulation of a significant amount of work between our federal government partners, especially the National Institute of Standards and Technology (NIST), and private stakeholders. I strongly support moving on the IoT cybersecurity label, and believe that it will ultimately help consumers identify how secure a device may be, and support safe networks. As we develop the proposal, however, I look forward to closely reviewing the record to make sure we get it right. I want to highlight two particular issues that are especially important.

First, it is vital that the cybersecurity label program is as pro-consumer as possible. We must ensure that our actions make it easier for consumers to quickly understand the information on the label and then make informed purchasing decisions. Along those lines, we properly ask critical questions to ensure that the cybersecurity labeling program matches consumer expectations. One important question is how the IoT cybersecurity labeling program should be scoped. Specifically, should it be focused on products as a whole, or on subcomponent devices. As we develop the record for guidance, it may also be useful for us to consider other successful government consumer education labeling programs, such as the Department of Energy's ENERGY STAR program. The item seeks comment on both approaches, and I will be closely reviewing the record to make sure we get this right. I thank the Chairwoman and my fellow Commissioners for agreeing to my edits to ensure that the IoT cybersecurity label has the proper scope.

Second, we must ensure that the IoT cybersecurity label protects Americans. If insecure equipment becomes included in the IoT cybersecurity label, it will undermine network security and the public's trust in the IoT cybersecurity labeling program. Thus, it is vital that we do not place our stamp of approval on devices from producers that the United States government and its agencies have already identified publicly as part of a national security review. I'm glad that the Chairwoman and my colleagues agreed to include a proposal to expand the list of products that will be excluded from access to the IoT cybersecurity label beyond the Commission's List of Covered Communications Equipment and Services to also include companies named on the Department of Commerce's Designated Entity List, the Department of Defense's List of Chinese Military Companies, and similar lists. I look forward to reviewing the record to further ensure that adversarial countries do not try to take advantage of the labeling program to harm our networks.

The Commission has recently taken strong steps to protect the security of our networks, and now, with the IoT cybersecurity label, connected products and devices. Last month, at my urging, the Commission for the first time explicitly required providers that deploy broadband networks receiving federal Universal Service funds to implement operational cybersecurity and supply chain risk management plans that reflect the latest NIST and government guidance. This ensured that networks built with Universal Service Fund support are just as secure as those built with other support programs from

[7] A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats, Action 5.2, Department of Commerce and Department of Homeland Security, May 22, 2018, *available at* https://www.commerce.gov/sites/default/files/2020-07/eo_13800_botnet_report_-_finalv2.pdf.

[8] Executive Order on Improving the Nation's Cybersecurity, Sec. 4, Enhancing Software Supply Chain Security, The White House, Executive Order 14028, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[9] National Cybersecurity Strategy, Strategic Objective 3.2, The White House, Mar. 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

other federal agencies. It is also an important precedent that will signal to other providers that they should do the same, if they haven't already done so. Combined with our efforts to protect connecting products and devices, we can be confident that we are taking important and necessary steps to secure our networks. But, there is more to do and I am committed to continuing to work with all stakeholders on any additional steps that we can take to protect our communications networks.

Those Carnegie Mellon students didn't know how their idea would flourish in the world when they just wanted a cold soda. Indeed, as they were creating the first IoT device, they joked around about how your toaster was one day going to be on the Internet.[10] Thanks to this proposal, we are one step closer to helping consumers understand exactly what cybersecurity protections their connected toaster, and many other IoT devices, have enabled. I thank the FCC staff that worked on this item for their hard work.

[10] *The Little Known Story of the First IoT Device*.