STATEMENT OF
COMMISSIONER GEOFFREY STARKS

Re: *Allowing Earlier Equipment Marketing and Importation Opportunities*, ET Docket No. 20-382, RM-11857.

This is a good commonsense proposal, and I look forward to the comments discussing how it should be implemented. Consumer expectations and the market for radiofrequency devices have evolved since the Commission first established its equipment marketing rules, and this NPRM proposes rule changes that update our policies to reflect those changes. But while we're updating our rules on these devices, it's appropriate to note another ongoing change regarding connected devices that also requires examination.

As I've noted before, the expansion of 5G technology will enable the interconnection of massive numbers of IoT devices. According to one study, the number of connected devices worldwide will increase from 9.1 billion in 2018 to more than 25 billion in 2025. Over 3 billion of these devices are expected to use wireless technology.[1] Networks of IoT devices could help reduce carbon emissions and waste, increase productivity, protect public safety, and generally enhance our way of life. At the same time, however, many of these devices originate overseas, including from adversary states like China. Thus, while we should recognize the potential advantages of these devices, we also must take measures to protect the privacy and security of our citizens.

The Commission and other policymakers need to engage on IoT security. Our critical infrastructure networks already contain these devices, and as governments and businesses incorporate smart technology into every aspect of our daily lives, the potential harm from a concerted attack will increase exponentially. Each device could be a potential entry point for a hostile actor to attack connecting networks.

More than four years ago, the world experienced the infamous Mirai cyberattack, in which hackers exploited vulnerabilities in connected devices like routers, surveillance cameras, and DVRs to launch coordinated DDoS attacks on web hosting service providers and journalists. The threat hasn't gone away. Earlier this month a technology news site found suspicious backdoors in affordable Chinese-made internet routers and Wi-Fi extenders sold at several major retailers that would allow an attacker to remotely control not only the devices, but also any devices connected to the same network. Further testing showed that these backdoors were not only potential threats, but that third parties were actively attempting to exploit them.[2]

Industry and government have taken some initial steps in this area. For example, several major telecom providers, tech companies and trade associations have formed a group to develop and advance industry consensus on baseline security capabilities for new devices.[3] The National Institute of Standards and Technology (NIST) has established its Cybersecurity for the Internet of Things program, which supports the development and application of standards, guidelines, and related tools to improve the

---

[1] *See* GSMA, *The GSMA Guide to the Internet of Things,* at 2 (Sept. 2018), *available at* https://www.gsma.com/iot/wp-content/uploads/2018/09/4048-GSMA-IOT-Guide2018-WEB.pdf.

[2] *See* "Walmart-exclusive router and others sold on Amazon & eBay contain hidden backdoors to control devices," Cybernews (Nov. 23, 2020), *available at* https://cybernews.com/security/walmart-exclusive-routers-others-made-in-china-contain-backdoors-to-control-devices.

[3] *See* Council for a Secure Digital Economy, "The C2 Consensus on IoT Device Security Baseline Capabilities" (Sept. 2019), *available at* https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf.

cybersecurity of connected devices and the environments in which they are deployed.[4] And just last month, the Senate unanimously passed Senator Warner's IoT Cybersecurity Improvement Act, which, among other things, requires NIST to issue cybersecurity standards for IoT devices and mandates that the federal government purchase only devices meeting those standards. The bill now awaits the President's signature.

But none of these actions address the inexpensive devices that are more likely to be manufactured and imported from adversary states like China and used by our most vulnerable businesses and consumers. The Commission should work with retailers to ensure that all equipment sold on their websites meet NIST security standards. Failing to do so risks harm not only to the consumers and businesses with insecure devices but to our broader networks as a whole. I look forward to continuing the discussion of this important issue.

Thank you to the staff of the Office of Engineering and Technology for their work on this item.

[4] *See* NIST Cybersecurity for IoT Program webpage (last updated Oct. 8, 2020), *available at* https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program.