TESTIMONY OF NATHAN SIMINGTON
COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION
BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY
OF THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE
COMMUNICATIONS & TECHNOLOGY SUBCOMMITTEE
"THE FISCAL YEAR 2025 FEDERAL COMMUNICATIONS COMMISSION AGENCY BUDGET"

JULY 9, 2024

SUMMARY OF TESTIMONY

- Securing wireless and IoT devices should be an urgent Commission priority.
- The Commission continues to divert resources to misguided, partisan priorities, ignoring urgent reforms like an overhaul of the Universal Service Fund.
- Foreign technology devices and services are increasingly used as vehicles for espionage and sabotage, specifically by China.
- I urge my colleagues to build further on the foundation the Commission recently built with the initial implementation of the US Cyber Trust Mark Program.

TESTIMONY OF NATHAN SIMINGTON

COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION

BEFORE THE SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

OF THE UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

COMMUNICATIONS & TECHNOLOGY SUBCOMMITTEE

"THE FISCAL YEAR 2025 FEDERAL COMMUNICATIONS COMMISSION AGENCY BUDGET"

JULY 9, 2024

Chairman Latta, Vice Chair Carter, Ranking Member Matsui, and distinguished Members of the Subcommittee, it is a privilege to appear before you today.

Today, I would like to address what I believe is one of the most pressing priorities for the Commission—securing wireless and Internet of Things (IoT) devices in the face of the accelerating move from a single Internet and technology market toward one fragmented along national borders due to concerns about digital sovereignty; specifically threats to the United States from China. Device security and technology evolution implicates all of the Commission's core functions at a basic level, specifically its authority over commercial spectrum.

However, before I highlight these concerns I must again express my frustration with the direction that the Commission has taken in dedicating its limited resources to implementation of partisan, unnecessary and burdensome policy frameworks, like the Title II broadband and digital

discrimination regulatory regimes. These heavy-handed priorities leave little room for commonsense, urgently needed reforms and invaluable Commission attention. Such reforms include not only a comprehensive framework for securing our networks from foreign threats, which I will address in detail, but also a Universal Service Fund contributions overhaul and a continued focus on space leadership.

But now to device security. There was a lot of idealism in the early days of the Internet. It was a universal, open network where people from around the world could exchange services and ideas basically without restriction. There were no borders online. If you put up a web site in the United States, someone on any other country could access it just as well, if a bit more slowly, than someone else in the US. Across the world, people were using the same devices, running the same software, usually with no more modification than a local translation of the user interface.

But today we have seen that there is potential for foreign technology devices and services to be vehicles for espionage and sabotage. We really cannot be sure that any non-trivial device from China, be it a network router or a laptop or a cellphone, can be trusted to not contain backdoors that would allow the Chinese government to exfiltrate data, take control of the device, or render it inoperative. But those same concerns must ultimately extend to any services that store data about Americans in adversary countries, or countries and companies that could easily come under the influence of those adversaries.

Even the most seemingly benign use of foreign technology can become a security threat. GPS, developed and controlled by the US military, was once the only satellite-based global

positioning and precision timing system in the world. But now it faces competition from foreign alternatives like the EU's Galileo, Russia's Glonass, and China's BeiDou. Supporting those systems is sometimes a requirement for device manufacturers wishing to sell in those countries. So between achieving economies of scale for manufacturers for all markets, and the fact that these positioning systems currently offer higher precision than the American GPS system, it appears that many American businesses and consumers are knowingly or unknowingly relying on these foreign systems in their operations.

And what's worse, American businesses and consumers often make the decision—most likely unknowingly—to buy untrustworthy equipment from Chinese or other foreign companies because they are inexpensive, or preselected by a preferred and trusted vendor. Unfortunately, most of these products come from companies that fail to take security seriously and that are careless in their software development practices. Companies like these routinely fail to correct known security vulnerabilities in a timely manner—and many don't even take the most basic precautions to prevent unauthorized access and control of the now millions of wireless and IoT devices they make available to these consumers and businesses.

Given all of these increasingly burgeoning threats, I am pleased that in March of this year, my Commission colleagues were willing to reach across the aisle and work diligently alongside me to put teeth into the Commission's implementation of the US Cyber Trust Mark program. This voluntary program sets 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. 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. And I look forward to continuing to work with colleagues to figure out how to expand this program to computers, smartphones, routers, and other devices.

My Commission colleagues also agreed to include a further notice of proposed rulemaking on the issue of how to handle devices that run 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—and as a result, there is still so much more work to be done.

* * *

Chairman Latta, Vice Chair Carter, Ranking Member Matsui, and Members of the Subcommittee, I want to thank you again for holding this hearing and for the opportunity to testify. I look forward to answering your questions.