FCC NEWS from the Federal Communications Commission

Media Contact:
Office of Media Relations
MediaRelations@fcc.gov

For Immediate Release

FCC CREATES VOLUNTARY CYBERSECURITY LABELING PROGRAM FOR SMART PRODUCTS

'U.S. Cyber Trust Mark' Program Will Help Consumers Make Informed Purchasing Decisions and Encourage Manufacturers to Meet Higher Cybersecurity Standards

WASHINGTON, March 14, 2024— The Federal Communications Commission today voted to create a voluntary cybersecurity labeling program for wireless consumer Internet of Things ("IoT") products. Under the program, qualifying consumer smart products that meet robust cybersecurity standards will bear a label—including a new "U.S Cyber Trust Mark"—that will help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards.

With today's action, the Commission has adopted the rules and framework for the program to move forward. Among program highlights:

- The U.S. Cyber Trust Mark logo will initially appear on wireless consumer IoT products that meet the program's cybersecurity standards.
- The logo will be accompanied by a QR code that consumers can scan for easy-to-understand details about the security of the product, such as the support period for the product and whether software patches and security updates are automatic.
- The voluntary program will rely on public-private collaboration, with the FCC providing oversight and approved third-party label administrators managing activities such as evaluating product applications, authorizing use of the label, and consumer education.
- Compliance testing will be handled by accredited labs.
- Examples of eligible products may include home security cameras, voice-activated shopping devices, internet-connected appliances, fitness trackers, garage door openers, and baby monitors.

The Commission is also seeking public comment on additional potential disclosure requirements, including whether software or firmware for a product is developed or deployed by a company located in a country that presents national security concerns and whether customer data collected by the product will be sent to servers located in such a country.

There are a wide range of consumer IoT products on the market that communicate over wireless networks. These products are made up of various devices, and are based on many technologies, each of which presents its own set of security challenges. Last August, the Commission proposed and sought comment on developing the voluntary cybersecurity labeling program for IoT. The rules adopted today are based on that record.

According to one third party estimate, there were more than 1.5 billion attacks against IoT devices in the first six months of 2021 alone. Others estimate that there will be more than 25 billion

connected IoT devices in operation by 2030. The cybersecurity labeling program builds on the significant public and private sector work already underway on IoT cybersecurity and labeling, emphasizing the importance of continued partnership so that consumers can enjoy the benefits of this technology with greater confidence and trust.

Action by the Commission March 14, 2024 by Report and Order (FCC 24-26). Chairwoman Rosenworcel, Commissioners Carr, Starks, Simington, and Gomez approving. Chairwoman Rosenworcel, Commissioners Starks, Simington, and Gomez issuing separate statements.

PS Docket No. 23-239

###