FCC NEWS from the Federal Communications Commission

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

For Immediate Release

CHAIRWOMAN ROSENWORCEL ADVANCES PLAN FOR CYBERSECURITY LABELING PROGRAM FOR SMART PRODUCTS

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

WASHINGTON, February 21, 2024—Federal Communications Commission Chairwoman Jessica Rosenworcel today announced that the Commission will vote at its March 14, 2024, Open Meeting on creating a voluntary cybersecurity labeling program for wireless consumer Internet of Things ("IoT") products.

Under the program, qualifying consumer smart products that meet cybersecurity standards would bear a label—including a new "U.S Cyber Trust Mark"—that would help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards. Eligible products may include home security cameras, voice-activated shopping devices, internet-connected appliances, fitness trackers, garage door openers, and baby monitors.

"Smart products can make our lives a lot more convenient but they can also pose security and privacy risks," **said Chairwoman Rosenworcel**. "This program would make it easier for consumers to choose more secure smart products for their homes, encourage companies to meet higher cybersecurity standards, and strengthen the ecosystem for connected products. Just as the ENERGY STAR program educated the public and created incentives for manufacturers to offer more energy-efficient appliances, our cybersecurity labeling program would pave the way to do the same with smart products."

If the program rules are adopted by a vote of the full Commission:

- The U.S. Cyber Trust Mark logo would appear on wireless consumer IoT products that meet baseline cybersecurity standards.
- The logo would be accompanied by a QR code that consumers can scan for easy-to-understand details about the security of the product, such as the guaranteed minimum support period for the product and whether software patches and security updates are automatic.
- The voluntary program would 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 would be handled by accredited labs.

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.

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 program that will be voted on next month was developed based on that record. The proposed new rules will be posted publicly on Thursday, February 22 at: www.fcc.gov/march-2024-open-commission-meeting.

###

Media Relations: (202) 418-0500 / ASL: (844) 432-2275 / Twitter: @FCC / www.fcc.gov