OFFICE OF THE CHAIRWOMAN

FACT SHEET: Securing Smart Devices

The FCC's Proposed Voluntary Cybersecurity Labeling Program for Internet-Enabled Devices

---

"There are now so many new devices—from smart televisions and thermostats to home security cameras, baby monitors, and fitness trackers—that are connected to the internet. These technologies provide huge benefits because they can make our lives easier and more efficient. But this increased interconnection brings more than just convenience; it brings increased security risk. That is why the Commission is proposing to put in place the first-ever voluntary cybersecurity labeling program for connected smart devices: The U.S. Cyber Trust Mark. Just like the "Energy Star" logo helps consumers know what devices are energy efficient, the Cyber Trust Mark will help consumers make more informed purchasing decisions about device privacy and security.
– FCC Chairwoman Jessica Rosenworcel

FACT SHEET

Overview

The Federal Communications Commission is seeking public comment on a proposal to create a voluntary cybersecurity labeling program that would provide consumers with clear information about the security of their internet-enabled devices, commonly called "Internet of Things" (IoT) or "smart" devices. The proposed program—where qualifying products would bear a new U.S Cyber Trust Mark—would help consumers make informed purchasing decisions, differentiate trustworthy products in the marketplace, and create incentives for manufacturers to meet higher cybersecurity standards.

The FCC's program would be similar to the Energy Star program, which was created to help consumers identify energy-efficient appliances and encourage more companies to produce them in the marketplace—but for more cybersecure smart devices.

Why the Program is Needed

There are a wide range of consumer smart products on the market that communicate over networks, running the gamut from personal digital assistants to internet-connected home security cameras, voice-activated shopping devices, internet-connected appliances, fitness trackers, GPS trackers, medical devices, garage door openers, and baby monitors. These products bring enormous benefits but also present a range of security challenges. According to one third-party estimate, there were more than 1.5 billion attacks against smart devices in the first six months of 2021 alone. Meanwhile the number of smart devices is skyrocketing, with some estimating that there will be more than 25 billion connected devices in operation by 2030.

How the Program Would Help Consumers

If the program is established, you would be able to easily identify smart devices and products that meet widely accepted security and privacy standards by looking for the U.S. Cyber Trust Mark logo. The logo would appear on packaging alongside a QR code that you could scan for more information. The QR code would link to a national registry of certified devices so that you could compare these devices and get the most and up-to-date security information about each.

The Commission expects that over time, an increasing number of manufacturers would participate in the voluntary program to demonstrate their commitment to privacy and security, as there would be increased consumer demand for easily identifiable trustworthy smart products.

Program Details

The FCC's proposal, called a Notice of Proposed Rulemaking, outlines the voluntary cybersecurity labeling program, which would be based on criteria developed by the National Institute of Standards and Technology (NIST). The proposal builds on and seeks to leverage the significant public and private sector work already underway on smart device cybersecurity and labeling, and it emphasizes the importance of continued partnership.

The proposal poses questions about how to create the most effective program, inviting public comment on issues including:

- The scope of devices or products for sale in the U.S. that should be eligible for inclusion in the labeling program,
- Who should oversee and manage the program,
- How to develop the security standards that could apply to different types of devices or products,
- How to demonstrate compliance with those security standards,
- How to safeguard the cybersecurity label against unauthorized use, and
- How to educate consumers about the program.

The FCC will evaluate the public input to determine next steps. If the FCC votes to establish the program, it could be up and running by late 2024.

###

Released: August 10, 2023

Media Contact: MediaRelations@fcc.gov