# United States to launch cybersecurity labelling programme for smart devices



The United States government is gearing up for the introduction of its cybersecurity labelling programme specifically aimed at consumer internet-connected devices, under the initiative named the Cyber Trust Mark. This programme, which was first unveiled in 2023, is anticipated to be "open for business" sometime this year, according to a recent announcement from the White House, as reported by TechCrunch.

The Cyber Trust Mark is designed as a voluntary label that aims to enhance device security by providing U.S. consumers with more detailed information regarding the security features of the products they purchase. This initiative encompasses a wide range of consumer-grade internet-connected devices, including smart refrigerators, microwaves, televisions, routers, home security cameras, smart speakers, and fitness trackers. These devices often pose security risks due to issues such as easily guessable default passwords and a lack of assurance regarding ongoing security updates.

While an exact launch date has yet to be established, the White House has indicated that companies will soon be able to submit their Internet of Things (IoT) products for testing to one of 11 approved entities to qualify for the Cyber Trust Mark. The availability of certified products is set to coincide with their introduction in retail outlets later this year, as per information provided by TechCrunch.

Support for this initiative has been robust, with major manufacturers and retailers like Amazon, Google, Best Buy, Samsung, and LG Electronics backing the programme. Alongside this effort, there exists the Connectivity Standards Alliance, which aims to streamline the certification process for manufacturers, thereby ensuring compliance with a variety of international regulations and standards through a singular evaluation process.

Previous analyses conducted by PYMNTS have highlighted the significance of these initiatives. For instance, the publication noted, “In essence, while the road to achieving comprehensive IoT security may be long, these efforts by major industry players and government bodies represent key milestones in establishing a robust security framework for the growing array of smart home gadgets available on the market today.” The report emphasised the importance of collaboration among stakeholders to effectively address cybersecurity issues and build consumer trust in the ever-expanding landscape of connected devices.

Recent statistics further illustrate the increasing penetration of smart technologies in consumer lifestyles. The PYMNTS Intelligence report titled “Multitasking Consumers Want to Shop — and Work — at the Same Time” indicates that the average consumer currently owns approximately six connected devices. This figure rises to seven for millennials and bridge millennials. Moreover, the prevalence of smart home devices is on an upward trajectory, with ownership of smart refrigerators growing from 5% in 2019 to 9% in 2023, while connected thermostat ownership saw an increase from 10% to 15% in the same timeframe.

These developments underscore the accelerating adoption of smart technologies and the evolving landscape of cybersecurity in relation to consumer devices, highlighting the dual focus on enhancing user convenience and improving device security.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/> - Corroborates the White House announcement of the U.S. Cyber Trust Mark program and its purpose.
2. <https://www.fcc.gov/CyberTrustMark> - Provides details on the FCC's Cyber Trust Mark program, including eligible products and the application process.
3. <https://www.fcc.gov/CyberTrustMark> - Explains the types of consumer wireless IoT products included in the program, such as home security cameras and smart appliances.
4. <https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/> - Mentions the involvement of accredited labs and Cybersecurity Label Administrators in the testing and certification process.
5. <https://www.fcc.gov/CyberTrustMark> - Details the process for manufacturers to apply for the U.S. Cyber Trust Mark, including testing by accredited labs and review by Cybersecurity Label Administrators.
6. <https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/> - Highlights the support from major manufacturers and retailers like Amazon, Best Buy, and others for the Cyber Trust Mark program.
7. <https://www.fcc.gov/CyberTrustMark> - Explains the public-private collaboration and the role of the FCC in overseeing the program.
8. <https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/> - Discusses the importance of the program in enhancing consumer trust and addressing cybersecurity issues in connected devices.
9. <https://www.fcc.gov/CyberTrustMark> - Lists the products not included in the program, such as medical devices, motor vehicles, and wired devices.
10. <https://www.whitehouse.gov/briefing-room/statements-releases/2025/01/07/white-house-launches-u-s-cyber-trust-mark-providing-american-consumers-an-easy-label-to-see-if-connected-devices-are-cybersecure/> - Mentions the conditional approval of 11 companies as Cybersecurity Label Administrators and the selection of UL Solutions as the Lead Administrator.
11. <https://www.fcc.gov/CyberTrustMark> - Provides information on the QR code and registry of information linked to the Cyber Trust Mark logo, detailing product security features.
12. <https://www.pymnts.com/cybersecurity/2025/cyber-trust-mark-program-smart-devices-set-go-live/> - Please view link - unable to able to access data