# White House launches U.S. Cyber Trust Mark for smart home devices



The White House, in collaboration with the Federal Communications Commission (FCC), is set to introduce a voluntary initiative titled the 'U.S. Cyber Trust Mark' for wireless smart home devices, a significant move designed to enhance cybersecurity standards within the burgeoning Internet of Things (IoT) market. This initiative mirrors the well-known Energy Star label but focuses specifically on the cybersecurity aspects of home automation products. The program is expected to launch in 2025, providing consumers with a clearer path to understanding the security levels of various devices.

The Cyber Trust Mark will allow manufacturers to display this label on their products, provided they successfully pass a cybersecurity assessment managed by the National Institute of Standards and Technology (NIST). This initiative aims to create a competitive incentive for manufacturers to improve device security, while simultaneously equipping consumers with vital information about the safety of the products they purchase. Each product bearing the mark will include a QR code on its packaging that, when scanned, will reveal essential security information pertaining to the device.

The details accessible via the QR code will outline critical aspects such as how to change the device's default password, guidance on securely configuring the device, information on automatic updates, and the minimum duration of support the manufacturer offers for security updates. Speaking to Android Police, the White House underscored the program's goal to help consumers make more informed purchasing decisions in a marketplace increasingly concerned with security vulnerabilities.

The initiative will focus solely on wireless IoT products such as smart appliances, security cameras, fitness trackers, and voice-activated devices, explicitly excluding wired devices, medical devices regulated by the FDA, personal computers, smartphones, and routers from eligibility. The FCC added that the framework for this program was laid down in March 2024 and is presently in the implementation phase, with further announcements expected prior to the opening of the application process in 2025.

The introduction of the Cyber Trust Mark comes as the interconnected nature of smart home devices continues to grow, providing unparalleled convenience but also raising security concerns that have prompted the government to take action. As more consumers incorporate these devices into their daily lives, the new mark aims to address fears surrounding vulnerabilities that could potentially compromise privacy and security.

With the launch of this initiative, the White House and FCC appear to be striving to strike a balance between technological advancement and consumer safety within the rapidly evolving landscape of smart home technology, while also preparing the market for a more transparent approach to product security in the years to come.

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

## Bibliography

1. <https://techcrunch.com/2025/01/07/us-government-set-to-launch-its-cyber-trust-mark-cybersecurity-labeling-program-for-internet-connected-devices-in-2025/> - Corroborates the introduction of the U.S. Cyber Trust Mark, its launch in 2025, and the program's focus on enhancing cybersecurity for internet-connected devices.
2. <https://www.betterworldtechnology.com/post/u-s-unveils-cyber-trust-mark-a-new-era-for-secure-devices> - Supports the initiative's aim to help consumers make informed choices about device security, the involvement of NIST standards, and the use of QR codes for security information.
3. <https://thehackernews.com/2025/01/fcc-launches-cyber-trust-mark-for-iot.html> - Confirms the role of the FCC, the use of NIST standards, and the details provided via QR codes, such as changing default passwords and automatic updates.
4. <https://techcrunch.com/2025/01/07/us-government-set-to-launch-its-cyber-trust-mark-cybersecurity-labeling-program-for-internet-connected-devices-in-2025/> - Details the comparison to the Energy Star label and the program's voluntary nature, as well as the support from major retailers like Best Buy and Amazon.
5. <https://www.betterworldtechnology.com/post/u-s-unveils-cyber-trust-mark-a-new-era-for-secure-devices> - Explains the cybersecurity assessment process managed by NIST and the competitive incentive for manufacturers to improve device security.
6. <https://thehackernews.com/2025/01/fcc-launches-cyber-trust-mark-for-iot.html> - Mentions the framework laid down in March 2024 and the ongoing implementation phase leading up to the application process in 2025.
7. <https://techcrunch.com/2025/01/07/us-government-set-to-launch-its-cyber-trust-mark-cybersecurity-labeling-program-for-internet-connected-devices-in-2025/> - Discusses the exclusion of certain devices like wired devices, medical devices regulated by the FDA, personal computers, smartphones, and routers from the program.
8. <https://www.betterworldtechnology.com/post/u-s-unveils-cyber-trust-mark-a-new-era-for-secure-devices> - Highlights the growing security concerns with smart home devices and the government's action to address these concerns through the Cyber Trust Mark.
9. <https://thehackernews.com/2025/01/fcc-launches-cyber-trust-mark-for-iot.html> - Details the future implications, including the expansion to enterprise devices and the executive order mandating federal agencies to purchase only certified devices starting in 2027.
10. <https://techcrunch.com/2025/01/07/us-government-set-to-launch-its-cyber-trust-mark-cybersecurity-labeling-program-for-internet-connected-devices-in-2025/> - Explains the focus on improving the security of routers used in small offices and home offices in the second phase of the initiative.
11. <https://www.betterworldtechnology.com/post/u-s-unveils-cyber-trust-mark-a-new-era-for-secure-devices> - Emphasizes the initiative's goal to empower consumers to make safer choices and to foster a more secure digital environment.
12. <https://www.androidpolice.com/smart-home-tech-cyber-trust-logo-mark/> - Please view link - unable to able to access data