TECHNET
THE VOICE OF THE INNOVATION ECONOMY

1420 New York Avenue NW, Suite 825
Washington, D.C. 20005
www.technet.org | @TechNetUpdate

October 6, 2023

Federal Communication Commission
Office of the Secretary
45 L Street, N.E.
Washington, D.C. 20554

Re: "In the Matter of Cybersecurity Labeling for Internet of Things" Proposed Rulemaking (*PS Docket No. 23-239*)

To Whom it May Concern:

TechNet appreciates the opportunity to provide comments on the Federal Communication Commission's ("FCC") notice of proposed rulemaking regarding cybersecurity labeling for Internet of Things (IoT) devices, referred to as the Cyber Trust Mark program. Given the complexity of this proposal, we urge the FCC to administer this program with a clear view of its responsibilities, limits, and authorities for doing so; ensure the process for assessing compliance with the proposed regulations are clear and unambiguous; and provide voluntary participants in the program with legal clarity regarding the potential liabilities or protections that arise from their participation.

TechNet is the national, bipartisan network of technology CEOs and senior executives that promotes the growth of the innovation economy by advocating a targeted policy agenda at the federal and 50-state level. TechNet's diverse membership includes dynamic American businesses ranging from startups to the most iconic companies on the planet and represents over 4.5 million employees and countless customers in the fields of information technology, artificial intelligence, e-commerce, the sharing and gig economies, advanced energy, transportation, cybersecurity, venture capital, and finance.

TechNet has long supported the adoption and use of voluntary, adaptable, risk management-based approaches to meet the cybersecurity needs of today's increasingly interconnected digital world. These principles include government participation, working through the National Institute of Standards and Technology (NIST) and the Office of the National Cyber Director, in the continued development of an international, consensus-driven IoT security guidance for consumer, industrial, and critical infrastructure. In addition, TechNet supports the creation of appropriate liability protections for organizations that participate in government cybersecurity sharing programs, as well as the avoidance of federal government

mandates on the design of products and services that could weaken the security of technology used to protect sensitive personal information and critical systems.

On May 12, 2021, President Biden issued Executive Order 14028, which directed NIST and the Federal Trade Commission to develop criteria for an IoT cybersecurity labeling program, which culminated in the release of NIST's Cybersecurity White Paper titled "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products" on February 4, 2022. We urge the FCC to devote the necessary resources and leverage collaboration with intergovernmental partners, such as NIST, to establish a program of this complexity. In addition, we urge the FCC to ensure that any process implemented to assess compliance with any adopted regulations does not unintentionally create cyber vulnerabilities or impose liability risks on participants in the voluntary program.

TechNet Comments

Compliance Assessment

First, we urge the FCC to align technical security criteria for the Cyber Trust Mark program with NIST IR 8425, a longstanding formal effort to develop IoT cybersecurity baseline guidance.[1] NISTIR 8425 allows for a range of methods for achieving common security goals, which will help the Cyber Trust Mark program requirements stay relevant and useful over time.

Such clarity will build on years of technical discourse between cybersecurity experts from industry, academia, and NIST, pursuant to statutory direction from Congress and Executive Orders from two Presidents. These baseline security measures constitute "reasonable" security for IoT devices in general and clear assurances from the FCC that the administration of the Cyber Trust Mark labeling program will be a strong partnership with manufacturers of IoT devices that will help achieve the primary objective of securing those devices.

Further, the FCC should ensure that any process implemented to assess compliance with any adopted regulations as part of the Cyber Trust Mark program does not create cyber vulnerabilities.

Incentives for Participation

In order to incentivize widespread participation in the Cyber Trust Mark program, TechNet urges the FCC to clarify the benefits for participation in the Cyber Trust Mark program and formally clarify that any IoT device that earns a Cyber Trust Mark label should be granted a "safe harbor" against federal and state enforcement

[1] National Institute of Standards and Technology Internal Report 8425, "*Profile of the IoT Core Baseline for Consumer IoT Products*" (September 2022)

actions and private civil litigation for alleged damages resulting from a cyber incident.

Conclusion

Thank you for your attention to our views on this matter. We appreciate the opportunity to submit comments and provide feedback on the Commission's proposed cybersecurity labeling program for IoT devices and stand ready to serve as a resource to you in the agency's implementation of this important program.

Sincerely,

Carl Holshouser
Senior Vice President