Cisco Systems, Inc.
601 Pennsylvania Ave. NW
Washington DC 20004

Phone: 202.354.2904
www.cisco.com

To: National Institute of Standards and Technology (NIST) (labeling-eo@nist.gov)

Re: DRAFT Baseline Security Criteria for Consumer IoT

Date: October 17, 2021

Cisco Systems, Inc. ("Cisco") is pleased to provide comments to the National Institute of Standards and Technology ("NIST") DRAFT Baseline Security Criteria for Consumer IoT, which was required by Executive Order (EO) 14028, "Improving the Nation's Cybersecurity." Cisco is the world's leading networking developer and manufacturer. We provide a comprehensive suite of products to support IoT connectivity.

Cisco thanks NIST for its leadership on this important problem and for the opportunity to offer these comments. We agree with much of the NIST paper. We would like to emphasize two points both pertaining to the recognition that any labeling program should not be limited to static information provided on a physical label at the time of purchase—and should facilitate automated network security post-purchase.

What happens the day after installation?

Particularly in the context of consumer goods, a manufacturer's responsibility for device cybersecurity cannot reasonably end on the day that the device is sold or first installed. After buying, one rarely looks at the label or the manual for an oven or a doorbell or a vacuum cleaner unless something has gone wrong. Static physical labels alone are not responsive to a dynamic threat environment. Consumers and—more importantly—the automated security tools they use

Cisco Systems, Inc.
601 Pennsylvania Ave. NW
Washington DC 20004

Phone: 202.354.2904
www.cisco.com

need to be aware of a device's posture **as and when it changes**. For that to happen, any physical label must be backed up by standardized, network-readable labels.

Similarly, when a person moves from one home to another—or devices are transferred from one owner to another—neither physical labels nor manuals are likely to be provided for most installed home IoT devices. These devices must first be automatically discoverable, so that the consumer can be made aware of their presence (and potential risk). This again demonstrates the importance of standardized, electronic information that can be used by networks to evaluate device capabilities and limitations and react accordingly.

Labels should provide not only posture information, but also information indicating whether the device is currently supported—and when that support will end. To address vulnerabilities discovered post-sale, manufacturers should also provide the simplest of upgrade instructions. The instructions should also be electronically available, so that any known mitigations are actionable.

Who is in a position to help consumers remediate risks?

On their own, consumers cannot reasonably be expected to remediate their IoT cyber-risks on an ongoing basis. Once IoT manufacturers are producing standardized electronically readable information, service providers, firewall vendors, and other security services will then be able to protect consumers by "reading" such labels, determining whether a device is vulnerable, and

Cisco Systems, Inc.
601 Pennsylvania Ave. NW
Washington DC 20004

Phone: 202.354.2904
www.cisco.com

prompting the owner with choices such as “upgrade” or “isolate.” Any labeling standard that enables those who in turn protect consumers will have provided a service to society.

Cisco supports the U.S. federal government’s efforts to improve the security of consumer IoT devices and commends NIST and its partner agencies leading the way for this development. Thank you for your consideration of our comments. Cisco looks forward to serving as a resource representing the technology industry’s perspective to NIST as it continues the important work of improving the nation’s cybersecurity posture. If you have any questions or would like to discuss our comments in greater depth, please contact us via the email addresses below.

Respectfully submitted,

Eliot Lear, Principal Engineer
ELear@cisco.com

Eric Wenger, Senior Director Technology Policy
ErWenger@cisco.com