Published on *The National Law Review* https://natlawreview.com

NIST Publishes New Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products

Article By:

Kristin L. Bryan

Marissa Black

On February 4, 2022, the National Institute of Standards and Technology ("NIST") published its Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products. These criteria make recommendations for cybersecurity labeling of consumer IoT products, i.e., those IoT products intended for personal, family, or household use.

NIST's guidance is yet another step forward in implementing the Biden Administration's May 2021 Executive Order on Improving the Nation's Cybersecurity. In that Executive Order, NIST was tasked with working with the Federal Trade Commission ("FTC") and others to identify a consumer labeling program for IoT. NIST's recommendations also include feedback obtained during an initial workshop in September 2021 and a second event in December 2021.

The purpose of these recommendations is to identify a potential labeling scheme—not to be established or managed by NIST—but rather by the scheme owner itself, which could be a public or private sector entity. These criteria are one step closer toward a national cybersecurity labeling scheme for consumer IoT products, and will likely be used as the model moving forward for these requirements.

The criteria established recommended considerations for three key aspects of a cybersecurity security IoT labeling program: (1) baseline product criteria; (2) labeling; and (3) conformity assessments.

With respect to baseline product criteria, NIST recommends an outcome-based approach that allows for the flexibility required by a diverse IoT marketplace. The outcome-based approach allows for solutions to be updated and changed over time without significant changes to the product criteria for labeling. The ten baseline criteria noted in the recommendations are: (1) asset identification; (2) product configuration; (3) data protection; (4) interface access control; (5) software update; (6) cybersecurity state awareness; (7) documentation; (8) information and query reception; (9) information dissemination; and (10) product education and awareness.

Next, NIST makes recommendations about label considerations. NIST recommends the use of a

binary label, that is, a single label indicating a product has met a baselines standard. In addition to the binary label, NIST suggests a “layered” approach, which would provide the consumer with additional details online via a URL or a scannable code (*i.e.*, a QR code). These labels should be available to consumers before purchase, at the time of purchase (in-store or online), and after purchase. NIST also emphasizes flexibility in supporting both digital and physical formats and encourages a robust consumer education campaign, including periodic testing with consumers to assess label appropriateness and usability.

The criteria also recommend considerations for a “conformity assessment” that would demonstrate a device’s compliance with the relevant standard. While a single conformity approach may not achieve desired outcomes, NIST lists three potential conformity assessment approaches: (1) self-attestation; (2) third-party testing and inspection; and (3) third-party certification.

National Law Review, Volumess XII, Number 49