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

NIST on Track to Release Draft Security Criteria for Consumer IoT Products

Article By:

Sheila A. Millar

Anushka N. Rahman

On August 31, 2021, the National Institute of Standards and Technology (NIST) released its draft white paper, *DRAFT Baseline Security Criteria for Consumer IoT Devices*. The draft white paper is in response to Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," which requires NIST, in collaboration with other agencies, to educate the public on Internet-of-Things (IoT) security. The draft white paper proposes baseline security criteria for consumer IoT products as part of a cybersecurity labeling program and builds on NIST's Secure Software Development Framework (SSDF) and other NIST documents. NIST is not establishing its own labeling program but instead seeks to identify minimum requirements for programs, which it must do by February 6, 2022.

NIST's summary sets out the timelines and objectives, along with some general principles. Labeling should:

- Encourage innovation in manufacturers' IoT security efforts, leaving room for changes in technologies and the security landscape.
- Be practical and not be burdensome to manufacturers and distributors.
- Factor in usability as a key consideration.
- Build on national and international experience.
- Allow for diversity of approaches and solutions across industries, verticals, and use cases – so long as they are deemed useful and effective for consumers.

The proposed labeling criteria set out in the draft white paper builds off of NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline and NISTIR 8259B, *IoT Non-Technical Supporting Capability Core Baseline*. NISTIR 8259B itself is new guidance released last month, and is intended to help manufacturers identify the non-technical capabilities they need to support device and system cybersecurity controls and to communicate with customers and third parties effectively. NISTIR

8259B is one of four documents recently released by NIST to help manufacturers and federal agencies manage cybersecurity, which include *IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements* (SP 800-213), *Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline* (NISTIR 8259C), and *Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government* (NISTIR 8259D).

NIST hosted an informative workshop on the proposed labeling criteria and related issues as previously announced on September 14–15. The workshop featured a variety of stakeholders, including representatives from federal agencies with experience in labeling programs, such as the Environmental Protection Agency (EPA), Federal Trade Commission (FTC) and Consumer Product Safety Commission (CPSC), as well as international experts. The workshop included discussions on how to define a "consumer," what should be in scope for a labeling program, limits of a labeling program, and achieving global harmonization, among many other topics. Recurring themes included assuring that a cybersecurity label avoids conveying a false sense of security and the need to keep labels simple.

Comments on the draft white paper are due October 17, 2021, and can be submitted to labeling-eo@nist.gov. NIST has already received feedback on important details, which were discussed during the workshop. With the growth of IoT devices, an IoT labeling scheme will likely have significant impact on many industry sectors, so interested stakeholders may wish to consider submitting comments.

National Law Review, Volumess XI, Number 259