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

NIST Lays Out Cybersecurity Guidance for Non-Technical Supporting Capabilities Related to IoT Devices

Article By:

Sheila A. Millar

Tracy P. Marshall

Anushka N. Rahman

With millions of Internet of Things (IoT) devices from phones to smart home censors flooding the market every year, effective cybersecurity to help mitigate risks to devices is vital. New guidance from The National Institute of Standards and Technology (NIST), *IoT Non-Technical Supporting Capability Core Baseline* (NISTIR 8259B), 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).

The guidance notes that “both device cybersecurity capabilities and non-technical supporting capabilities are vital to customers’ abilities to achieve their needs and goals.” While IoT devices are typically secured through technological capabilities, NISTIR 8259B focuses on the non-technical supporting capabilities that “that manufacturers or third parties take in support of the initial and ongoing security of IoT devices.” The guidance identifies four primary non-technical areas of cybersecurity:

- Documentation, which ensures that customers and third parties have the information they need to ensure their device and its data are secure;
- Information and query reception, which helps businesses respond to questions customers and others may have about a device’s security and operation;
- Information dissemination, which ensures that customers are kept in the loop about any newly discovered security issues or device or related systems updates; and

- Education and awareness, to assist customers and others in understanding how to secure and protect IoT software, hardware, and systems.

The guidance contains several tables that lay out detailed steps of common actions for organizations to consider taking and encourages organizations to add other non-technical capabilities where needed. NIST also updated its IoT catalog for device technical cybersecurity capabilities and supporting non-technical capabilities.

As IoT devices continue to rise in popularity, it is vital for manufacturers to ensure that their products come designed not only with effective cybersecurity technology but a plan for communicating with customers and third parties, keeping detailed records, and efficient methods for responding to questions. NISTIR 8259B gives organizations a helpful place to start, and this and other NIST guidance on IoT security may be relevant to the ongoing NIST cybersecurity labeling initiative.

National Law Review, Volume XI, Number 264