# Manufacturing “Smart” Devices? NIST Security Has Recommendations

Aaron J. Burstein

February 17, 2020

Regulatory interest in Internet of Things (“IoT”) devices is growing, partly in response to concerns about device security. In January, for example, California’s IoT Law (SB 327) went into effect. This law requires manufacturers of IoT devices to equip the devices with reasonable security features appropriate to the nature and function of the device, the information it may collect or transmit, protect the device and the consumer PII it contains from unauthorized access or disclosure.

In addition, at the federal level last year at least one bill was introduced addressing the cybersecurity of IoT devices: The Internet of Things Cybersecurity Improvement Act of 2019. Although the bill is being held in committee and will only directly affect federal IoT technology, it calls for the National Institute of Standards and Technology (NIST) to IoT-related security standards and guidelines.

In light of these developments, IoT device manufacturers would be “smart” to pay close attention to NIST’s draft *Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline* (the “Draft Recommendations”). The Draft Recommendations are described as voluntary, but various federal agencies, including the FTC, review and consider NIST publications in assessing privacy and data security practices.

NIST’s Draft Recommendations outline cybersecurity practices that manufacturers should consider adopting before they sell IoT devices to customers. According to NIST, these practices can help reduce the prevalence and severity of IoT device compromises (and attacks that exploit compromised IoT devices).

NIST’s Draft Recommendations consist of the following practices and further questions to help manufacturers and their customers to help address cybersecurity risks:

- **Identify expected customers and define expected use cases for IoT devices**.
    - *Which types of people or organizations are expected customers for the device?*
    - *How will the device be used?*
    - *Where, geographically, will the device be used?*
    - *What physical environments will the device be used in? (i.e. inside or outside, moving or stationary?)*
    - *What dependencies on other systems will the device need?*
    - *How might attackers misuse the device?*

- **Research customer cybersecurity goals**.
    - *How will the device interact with the physical world?*
    - *How will the device be managed, accessed, and monitored by the customer or other devices?*
    - *How will the cybersecurity measures affect the device's availability, efficiency, or effectiveness?*
    - *What data will the device store or transmit?*
    - *What are the sector-specific or legal regulations of the device?*
    - *What complexities will be introduced by the device interacting with other devices, systems, and environments?*
- **Determine how to address customer goals**. NIST defines a core cyber-capability baseline in furtherance of this goal through:
    - *Device Identification: specify how devices can be uniquely identified;*
    - *Device Configuration: ensure device firmware and software is protected from unauthorized access and modification;*
    - *Data protection: protect data that is stored and transmitted;*
    - *Logical Access to Interfaces: restrict logical access to local network interfaces to authorized entities only;*
    - *Software and Firmware Updates: ensure that updates can only be made by authorized entities; and*
    - *Cybersecurity State Awareness: create devices that can report on their cybersecurity state and make that information available to authorized entities only.*
- **Define approaches for communicating with customers**.
    - *What terminology will the customer understand?*
    - *How much information will the customer need?*
    - *How/where will the information be provided?*
    - *How can the integrity of the information be verified?*
- **Decide what to communicate to customers and how to communicate it**. NIST suggests answering the following questions for the customer:
    - *How long do you intend to support the device?*
    - *When do you intend for the device end-of-life to occur?*
    - *What functionality, if any, will the device have after support ends and the end-of-life?*
    - *How can customers report suspected problems with cybersecurity implications and how*

*will the manufacturer deal with these reports?*

Given the shifting legal landscape for IoT cybersecurity, adopting the practices and procedures in NIST's Draft Recommendations could protect a manufacturer's investment in this technology into the future.

---

Please join partner Alysa Hutnik for Privacy 101, a webinar that walks through topics such as:

- Privacy law 101
- Data security and breaches
- E-Mail, calls, and text marketing

**Register Here**