Atlantic Council

Security in the Billions

Toward a Multinational Strategy to Better Secure the IoT Ecosystem

Patrick Mitchell, Liv Rowley, and Justin Sherman
with Nima Agah, Gabrielle Young, and Tianjiu Zuo

Implementation for the United States

The purpose of this is to demonstrate how the United States should act to help develop a multinational strategy to better secure the IoT ecosystem.

Tier 1. Set the Baseline of Minimally Acceptable Security:

In comparison to other jurisdictions, the United States has preferred a less interventionist approach. There are two main exceptions: the two states that have enacted legislation to impose minimum security standards on IoT products, as well as the IoT Cybersecurity Improvement Act of 2020 which requires federal agencies to only procure devices that meet NIST security guidelines. In this context, the team recommends:

- **States should pass and enforce their own IoT security laws.** California and Oregon led the way but should expand their laws to focus on more specific guidance for organizations and manufacturers less versed in cybersecurity, rather than just focusing on concepts like "reasonable security." Ideally, they will do so in a way that does not lock in specific security measures into legal text but instead points toward another regulatory mechanism that more easily updates standards, such as the UK's approach of empowering an agency to maintain these standards, or points them to guidelines set for federal government agencies by NIST. More states should follow in their footsteps, putting forth IoT security laws that incorporate the standards outlined by the US government, as well as considering standards established by others around the world. The states that have implemented these laws should also study their impact. It is not apparent that any enforcement actions have yet occurred, which indicates one of two possible scenarios: all devices sold in their markets are now compliant, or enforcement has been insufficient. The latter seems more likely than the former.
- **The federal government should adopt the binary labeling approach proposed by NIST**. In NIST's February 2022 publication "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products," the organization recommends pursuing a binary labeling approach.[1] In this scenario, there would exist a single label stating that a product has met baseline security standards. Implementing the binary label would be a first step towards goals such as defining minimum security standards, creating and implementing a labeling program, and starting to broadcast to consumers what they should be looking for when purchasing IoT products. Among other details, this will require identifying an owner for the program, and the FTC would be the strongest candidate.

Tier 2. Incentivize Above the Baseline:

[1] NIST, "Recommended Criteria for Cybersecurity Labeling."

President Biden's 2021 Executive Order 14028 (Improving the Nation's Cybersecurity) directed NIST to design a labeling program for IoT devices, which should also serve as a mechanism to encourage the adoption of security measures that exceed the minimum baseline. The program's ultimate owner should:

- **Provide incentives for industry to obtain labels**. The US may look to Singapore and other countries that have adopted labeling programs to see how companies have been encouraged to participate in a labeling program and reach for higher tiers. Fee waivers for label applications may be a good way of incentivizing participation during the first few years of the program. Industry would likely react positively to some form of compensation for the third-party testing required to earn a higher label.
- **Provide liability protection for firms that pursue the higher, tier 2 security standards**. Experts have indicated that many players in industry would be incentivized to pick up higher security standards in exchange for liability protections. There are various types of liability protections that may be considered here, and this report leaves such determination up to the regulatory body. The implementation of such liability protection may take the form of a law passed by Congress outlining these protections, or conversely may come in the shape of a publicly articulated approach by the FTC.