Matthew J. Eggers
Vice President, Cybersecurity Policy | U.S. Chamber of Commerce
NEMA Annual Meeting | November 7, 2019
Cybersecurity Public Policy

BUY STRONG INTERNET OF THINGS (IOT) COALITION

Background: Security, Business, and Policy

The U.S. Chamber is exploring the creation of a Buy Strong IoT Coalition. The group would advance smart public policies in this space and promote the production and deployment of secure IoT products at home and abroad.[1]

The Chamber and the coalition would convene discussions with multiple stakeholders to frame key problems and sell a solution(s) to a broader audience. The coalition would shape the development and implementation of the IoT cyber baseline, which is being created by the National Institute of Standards and Technology (NIST)[2] in partnership with the business community, particularly the Council to Secure the Digital Ecosystem (CSDE).[3]

A top coalition priority would be to drive industry consensus on the technical criteria that underpin the IoT cyber baseline. The coalition would leverage this core baseline to advocate for approaches to IoT device security that align with the interconnected nature of the international marketplace.

Key Chamber Actions to Advance Security and Reduce Policy Fragmentation

- Engaging Congress on IoT cyber legislation since 2017. (November 2017, July 2019)
- Testifying before the Senate Commerce Committee on IoT cyber. (April 2019)
- Partnering with NIST in on the public-private core baseline for IoT devices. (October 2018, September 2019)
- Supporting the industry-driven CSDE C2 Consensus. (September 2019)
- Pressing foreign partners (e.g., the EU) to align their policies to the IoT cyber baseline.

Legislative Catalysts (Examples)

- **Sens. Mark Warner (D-VA) and Cory Gardner (R-CO)—Internet of Things Cybersecurity Improvement Act of 2019 (S. 734).** This legislation passed the Senate Homeland Security and Governmental Affairs Committee (HSGAC) in June 2019. The bill would mandate minimum security standards for IoT devices purchased by the federal government. It would also codify the NIST core baseline.

[1] The 2018 *Botnet Road Map* calls for establishing robust markets for consumer and industrial devices. The Chamber wants the IoT ecosystem to benefit from businesses leading the development of cutting-edge devices and risk management activities. The coalition would facilitate a process in the marketplace that generates both security and value for buyers and sellers.

[2] Draft NISTIR 8259, *Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers* (July 2019).

[3] *C2 Consensus on IoT Security Baseline Capabilities* (September 2019).

- **California state Sen. Hannah-Beth Jackson (D-19)—IoT device security law (S.B. 327).** Beginning on January 1, 2020, this law would require a manufacturer of a connected device to equip the device with a "reasonable" security feature(s) that are appropriate to the nature and function of the device and suitable to the information it may collect, contain, or transmit, among other stipulations. S.B. 327 is not alone. Many other states have taken up the IoT security baton, creating the potential for increased policy fragmentation.

- **Sen. Edward Markey (D-MA)—Cyber Shield Act of 2019 (S. 2664).** This bill, introduced in October 2019, would require the Commerce secretary to create a "voluntary program" to identify and certify IoT devices through labeling and other means of communicating about covered products that meet certain cybersecurity and data security benchmarks.

Federal IoT Security Legislation (Preemption): Looking to Ohio for Ideas

In September 2019, the Chamber wrote to NIST to support NISTIR 8259 and the C2 Consensus. We said that cyber stakeholders should increasingly direct their activities toward fostering market demand for strong devices and pressing public officials at home and internationally to align their policies to the industry-driven baseline. The Chamber stressed that policymakers need to match industry's leadership concerning IoT standards development, device security, and resilience. IoT cyber legislation needs to be passed that reflects the baseline, protects device makers and buyers, reduces policy fragmentation globally, and bolsters collective defense.

The legal liability protection that the Chamber is considering for device makers and purchasers is inspired by the Cyber SAFETY Act and the Ohio Data Protection Act (S.B. 220).[4] There is general agreement among the Chamber's Cybersecurity Working Group (CWG) that a revised version of S.B. 220—informally dubbed Ohio+—could serve as a model for negotiating a preemptive IoT cyber bill vis-à-vis the Senate Commerce, Science, and Transportation Committee.

Ohio+: A Snapshot

Various states and associations, including the state of Ohio and the Conference of Western Attorneys General (CWAG), have been developing model legislation that would provide businesses with some measure of protection from legal liability if it (1) is victimized by a third-party breach but (2) has voluntarily made reasonable and timely investments in its cybersecurity.

The Ohio law, passed in 2018, serves as a viable prototype for future model legislation. Ohio+ puts forward a data security/cybersecurity safe harbor that reasonably addresses the concerns of both business owners and policymakers who wish to encourage industry to proactively invest in their organizations' cyber programs.

[4] A good analysis of S.B. 220 is provided by The Ohio State University and the Cleveland State University colleges of law (March 2019).

Currently, such negotiations are taking place (very slowly) in the context of national privacy legislation, not IoT. Senate Commerce Committee staff suggest that privacy legislation will need to be addressed before IoT security legislation can be taken up in a meaningful way.

Three Main Takeaways

- **Industry and NIST leadership.** The business community, NIST, and other stakeholders are developing a security baseline for IoT devices.

- **A win-win cybersecurity market.** The Chamber wants device makers, service providers, and buyers to gain from the development of state-of-the-art IoT components and sound risk management practices.

- **Global, industry-driven standards and practices.** The Chamber believes that IoT cyber efforts will be most effective if they reflect global standards and industry-driven practices. A fragmented global cybersecurity environment creates uncertainty for industry and splinters the resources that businesses devote to device development, production, and assessments.