ASSOCIATED INDUSTRIES OF MASSACHUSETTS

1 Beacon Street, 16th Floor
Boston, MA 02108
www.aimnet.org | 617.262.1180 | fax 617.536.6785

July 18, 2017

**STATEMENT OF ASSOCIATED INDUSTRIES OF MASSACHUSETTS BEFORE HOUSE CHAIR JOSEPH F. WAGNER, SENATE CHAIR ERIC P. LESSER, AND MEMBERS OF THE JOINT COMMITTEE ON ECONOMIC DEVELOPMENT AND EMERGING TECHNOLOGIES IN OPPOSITION TO S.179, AN ACT RELATIVE TO THE CYBERSECURITY OF THE INTERNET OF THINGS AND OTHER SMART DEVICES.**

Good Afternoon, for the record my name is Bradley A. MacDougall, Vice President for Government Affairs at Associated Industries of Massachusetts (AIM).

AIM is opposed to S.179, An Act relative to the cybersecurity of the internet of things and other smart devices.

AIM believes that data security and protection of individual's personally identifiable information is critical. However, on behalf of AIM's 4,000 members, we wish to express strong concerns with S.179 and other recent state legislative proposals governing the "Internet of Things" (IOT) and believe that this committee and legislature should reject these proposals.

AIM urges policy makers to retain a welcoming statutory and regulatory environment for the Internet of Things (IOT), which is an emerging and constantly growing area driven by consumer demand and entrepreneurial activity. Massachusetts is currently home to and can be home to many new innovative technologies and start-up companies that leverage the power of the internet and devices.

Massachusetts should not only be the home of startups, manufacturers, software and device manufacturers in addition to and globally recognized firms that develop (IOT) technologies, we should be a state that encourages growth, investment and encouraging those companies to put their headquarters, jobs and investments in the Commonwealth.

To this end, AIM does support a national strategy on the internet of things that provides the necessary protections related to the collection of information while continuing to encourage both entrepreneurial and consumer innovation in the expansive area of technology.

As this committee reviews this legislation, members should be aware that AIM and our members were leading voices in the promulgation of state regulations 201 CMR 17.00 and a leader in supporting the business community's adoption of the nation's most comprehensive cybersecurity statutes 93H and 93I, relative to the protection of individual's personally identifiable information. These regulations authorized by 93H took three year to promulgate.

The challenge for Massachusetts policy makers is that the federal government has and continues to work on coordinating regulatory structures around this expansive area of technology and innovation. Among other federal agencies, the Food and Drug Administration, the Federal Communications Commission, the Federal Trade Commission and the National Highway Traffic Security Administration have authority to regulated IOT technologies. Also the National Institute of Standards and Technology as well as the Commerce Department have been wrestling with how define the IOT landscape and seeking public comments on how the federal government should regulate IOT. Also, today, the National Telecommunications and Information

Administration within the U.S. Department of Commerce is hosting a virtual meeting titled "Multistakeholder Process on Internet of Things Security Upgradability and Patching".[1]

These federal agencies are working together to create a national privacy framework across all companies in the internet ecosystem. In an effort to avoid a patchwork of legislation and in order to ensure regulatory consistency for all industries balanced with necessary and appropriate protections for consumers, we urge that the Committee refrain from action on this complex issue.

Regarding the specifics of the legislation, S.179 proposes to amend MGL 93H by adding definitions such as "Internet of Things (IOT)" and "IOT Personal Data". These definitions are ones that the federal government has and continues to struggle with. The term "internet of things" is extremely vast. The pace of IOT development is so fast that definitions are likely to become outdated or least inconsistent with federal standards.

Also the regulatory aspect of S.179 is challenging since any regulatory structure for driverless cars, a Fitbit, insulin pump, defibrillator, home heating or security systems, robots, and other home appliances can be very different.

AIM appreciates the committee's consideration of this testimony**.** Should you have any questions, please contact me directly at 617-262-1180.

[1] https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security