SENATE DOCKET, NO. 851 FILED ON: 1/16/2019

SENATE . . . . . No. 1887

The Commonwealth of Massachusetts

PRESENTED BY:

Michael O. Moore

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act establishing a Cybersecurity Control and Review Commission.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	
Michael O. Moore	*Second Worcester*	
Rebecca L. Rausch	*Norfolk, Bristol and Middlesex*	*1/30/2019*

SENATE DOCKET, NO. 851 FILED ON: 1/16/2019

SENATE . . . . . No. 1887

By Mr. Moore, a petition (accompanied by bill, Senate, No. 1887) of Michael O. Moore and Rebecca L. Rausch for legislation to establish a Cybersecurity Control and Review Commission. State Administration and Regulatory Oversight.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-First General Court
(2019-2020)

An Act establishing a Cybersecurity Control and Review Commission.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. "Critical Data" refers to private information held by state agencies and private sector companies. This can include, but is not limited to: names, health records, credit reports, credit card numbers, sealed court records, addresses, etc.

"Critical Infrastructure" refers to the systems and assets within the commonwealth, either physical or virtual, so vital to the commonwealth or the United States that the incapacitation or destruction of such systems would have a debilitating impact on physical security, economic security, public health or safety, or any combination of those matters. This can include, but is not limited to: election systems, transportation infrastructure, water, gas, and electric utilities.

"Cyber Attack" refers to an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; or destroying the integrity of the data or stealing controlled information.

"Cyber Incident" refers to actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein.

"Cybersecurity" refers to the process of developing and implementing both protections against cyber attacks and methods to respond and recover in the event of a successful cyber attack.

"Cyber System" refers to the network of hardware, software, procedures, and people put in place by companies, individuals, or governments that can connect to the Internet.

"Cyber Secure" refers to the state where a cyber system is prepared to the best of known technical ability to withstand the majority of known cyber attacks.

SECTION 2. There is hereby established a Cybersecurity Control and Review Commission to consist of 13 members. Said commission shall be comprised of the Secretary of Technology Services and Security, or his designee, who shall serve as chair. The Commission shall include the secretary of public safety and security, or his designee; one Senator appointed by the Senate President; one Senator appointed by the Senate Minority Leader; one Representative appointed by the Speaker of the House of Representatives; one Representative appointed by the House Minority Leader; and one representative from the Massachusetts Municipal Association. The Governor shall 8 members with relevant subject matter expertise, including one member with cybersecurity subject matter expertise from each of the following industries: healthcare, banking, utilities, academia; and a general cybersecurity expert.

SECTION 3. (a) The Commission shall recommend standards for interagency cybersecurity data collaboration between private and state agencies. The Commission shall also

determine standards for state hardware and software acquisitions, state employee cybersecurity training, and protection of state data. The Commission shall base these standards off the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CF).

(b) The Commission shall make its determined cybersecurity standards available to businesses operating within the Commonwealth. The Commission shall create a process for cybersecurity accreditation for businesses which have a demonstrated pattern of following the cybersecurity standards within the business's cybersecurity procedures.

(c) Any private sector business contracted with state agencies; or handling critical infrastructure or critical data; shall be required to adopt the Commission's standards for its specific sector.

(d) The Commission shall tailor their recommendations to the five specific industries with representatives on the Commission. Businesses and state agencies operating within each sector will only be responsible for implementing the specific cybersecurity standards related to their sector. The Commission will also produce generalized recommendations that all private and public sector agencies are recommended or required (see above) to follow.

SECTION 4: (a) The Commission shall submit a report to both the Special Senate Committee on Cyber Security and the Massachusetts State Legislature no later than December 1 each year, describing recommendations to ensure the sustainability of the Commonwealth's critical infrastructure and data protection cybersecurity standards and preparedness.

(b) The report submitted by the Commission to the Massachusetts State Legislature is confidential.

(c) The Commission shall condense and redact the information in the report into a publically viewable document by December 31 of the year in which the report is submitted.