SENATE DOCKET, NO. 399 FILED ON: 1/29/2021

SENATE . . . . . No. 2088

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*	
Tami L. Gouveia	*14th Middlesex*	*6/9/2021*
Maria Duaime Robinson	*6th Middlesex*	*7/22/2021*
Marc R. Pacheco	*First Plymouth and Bristol*	*7/22/2021*

SENATE DOCKET, NO. 399 FILED ON: 1/29/2021

SENATE . . . . . No. 2088

By Mr. Moore, a petition (accompanied by bill, Senate, No. 2088) of Michael O. Moore for legislation to establish a Cybersecurity Control and Review Commission. State Administration and Regulatory Oversight.

[SIMILAR MATTER FILED IN PREVIOUS SESSION
SEE SENATE, NO. *1887* OF 2019-2020.]

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Second General Court
(2021-2022)

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:

Chapter 6 of the General Laws is hereby amended by adding the following section:-

Section 220. (a) For purposes of this section, the following words shall have the following meanings:

"Critical data", private information held by state agencies and private sector companies, including, not limited to, names, health records, credit reports, credit card numbers, sealed court records and addresses.

"Critical infrastructure", the systems and assets, either physical or virtual, within the commonwealth that are so vital to the commonwealth or the United States that the incapacitation or destruction of such a system or asset would have a debilitating impact on physical security,

economic security, public health or safety or any combination thereof; provided, however, that "critical infrastructure" shall include, but not be limited to, election systems, transportation infrastructure, water, gas and electric utilities.

"Cyber attack", an attack via cyberspace that targets an enterprise's use of cyberspace to disrupt, disable, destroy or maliciously control a computing environment or infrastructure, destroy the integrity of the data or steal controlled information.

"Cyber incident", action taken through the use of an information system or network that results in an actual or potentially adverse effect on an information system, network or the information residing therein.

"Cybersecurity", 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", the network of hardware, software, procedures and people put in place by a company, individual or government that can connect to the Internet.

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

(b) There shall be a cybersecurity control and review commission.

The commission shall consist of: the secretary of technology services and security or a designee, who shall serve as chair; the secretary of public safety and security or a designee; 1 member appointed by the Massachusetts Municipal Association, Inc.; and 12 members appointed by the governor who shall have relevant subject matter expertise, 1 of whom shall have cybersecurity subject matter expertise in healthcare, 1 of whom shall have cybersecurity subject

matter expertise in banking, 1 of whom shall have cybersecurity subject matter expertise in utilities, 1 of whom shall have cybersecurity subject matter expertise in academia and 1 of whom shall be a general cybersecurity expert.

(c) The commission shall recommend standards for: (i) interagency cybersecurity data collaboration between private and state agencies; and (ii) state hardware and software acquisitions, state employee cybersecurity training and protection of state data. The standards shall be based on the National Institute of Standards and Technology Cybersecurity Framework. All private and public sector agencies may have to follow the general cybersecurity recommendations as well as applicable sector-specific recommendations for healthcare, banking, utilities or academia. Businesses and state agencies operating within a specific sector shall only be required to implement the cybersecurity standards applicable to their sector. The standards shall be made available to businesses operating within the commonwealth.

(d) The commission shall create a process for cybersecurity accreditation for businesses that have a demonstrated pattern of following the cybersecurity standards within the business' cybersecurity procedures.

(e) Any business that contracts with state agencies or handles critical infrastructure or critical data shall be required to adopt the commission's standards for its specific sector.

(f) Annually, not later than December 1, the commission shall submit a confidential report to the special senate committee on cyber security and the clerks of the house of representatives and the senate that contains recommendations to ensure the sustainability of the commonwealth's critical infrastructure and data protection cybersecurity standards and preparedness.

(g) Annually, not later than December 31, the commission shall make a condensed and redacted version of the report available to the public.