

**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:	
<i>Michael O. Moore</i>	<i>Second Worcester</i>	
<i>Rebecca L. Rausch</i>	<i>Norfolk, Bristol and Middlesex</i>	<i>1/30/2019</i>

**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:*

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

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

9 “Cyber Attack” refers to an attack, via cyberspace, targeting an enterprise’s use of  
10 cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a  
11 computing environment or infrastructure; or destroying the integrity of the data or stealing  
12 controlled information.

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

16 “Cybersecurity” refers to the process of developing and implementing both protections  
17 against cyber attacks and methods to respond and recover in the event of a successful cyber  
18 attack.

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

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

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

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

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

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

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

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

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

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

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