

**SENATE . . . . . No. 32**

---

**The Commonwealth of Massachusetts**

\_\_\_\_\_

PRESENTED BY:

***Barry R. Finegold***

\_\_\_\_\_

*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 relative to cyber incident response.

\_\_\_\_\_

PETITION OF:

NAME:

*Barry R. Finegold*

DISTRICT/ADDRESS:

*Second Essex and Middlesex*

**SENATE . . . . . No. 32**

---

By Mr. Finegold, a petition (accompanied by bill, Senate, No. 32) of Barry R. Finegold for legislation relative to cyber incident response. Advanced Information Technology, the Internet and Cybersecurity.

---

**The Commonwealth of Massachusetts**

\_\_\_\_\_  
**In the One Hundred and Ninety-Third General Court  
(2023-2024)**  
\_\_\_\_\_

An Act relative to cyber incident response.

*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. Chapter 7D of the General Laws, as appearing in the 2022 Official Edition,  
2 is hereby amended by inserting after section 11 the following new sections:-

3 Section 12. State-Level Incident Reporting and Response

4 (a) As used in this section and section 13, the following words shall have the following  
5 meanings, unless the context clearly requires otherwise:

6 “Breach of security” shall have the same meaning as defined in section 1 of chapter 93H.

7 “Critical infrastructure”, the systems and assets, either physical or virtual, within the  
8 commonwealth that are so vital to the commonwealth or the United States that the incapacitation  
9 or destruction of such a system or asset would have a debilitating impact on physical security,  
10 economic security, public health or safety or any combination thereof; provided, however, that

11 “critical infrastructure” shall include, but not be limited to, election systems, transportation  
12 infrastructure, water, gas and electric utilities.

13 “Cybersecurity incident”, an incident that: (i) risks or could risk the confidentiality,  
14 integrity or availability of information systems; (ii) consists of unauthorized access to, or  
15 malicious software present on, systems or assets that are so vital that the incapacity or  
16 destruction of such systems or assets would have a debilitating impact on cybersecurity, physical  
17 security, economic security, public health or public safety; and (iii) results or could result in a  
18 significant loss of data, system availability or control of systems; provided, however, that a  
19 “cybersecurity incident” shall include, but not be limited to, a breach of security, imminent threat  
20 of a breach of security or other cyber attack intended to compromise the use of an electronic  
21 system.

22 “Cybersecurity threat”, an action on or through an information system that may result in  
23 an unauthorized effort to adversely impact the security, availability, confidentiality or integrity of  
24 an information system or information that is stored on, processed by or transiting an information  
25 system; provided, however, that a “cybersecurity threat” does not include any action that solely  
26 involves a violation of a consumer terms-of-service agreement or consumer licensing agreement.

27 “Response team”, the Massachusetts Cyber Incident Response Team established pursuant  
28 to this section.

29 (b) There shall be established a Massachusetts Cyber Incident Response Team, the  
30 mission of which is to enhance this commonwealth’s ability to prepare for, respond to, mitigate  
31 against and recover from significant cybersecurity incidents.

32 (c) The response team shall consist of: (i) the secretary of the executive office of  
33 technology services and security or their designee, who shall serve as chair of the response team;  
34 (ii) a representative of the commonwealth security operations center as designated by the director  
35 of security operations; (iii) the secretary of the executive office of public safety and security or  
36 their designee; (iv) a representative of the state police cyber crime unit; (v) a representative of  
37 the commonwealth fusion center; (vi) the adjutant general of the Massachusetts National Guard  
38 or their designee; and (vii) the director of the Massachusetts emergency management agency or  
39 their designee.

40 (d) The response team shall review cybersecurity threat information and vulnerabilities,  
41 make informed recommendations and establish appropriate policies to manage the risk of  
42 cybersecurity incidents for all state agencies served by the executive office of technology  
43 services and security; provided, however, that such recommendations, policies and directives  
44 shall be informed by information and best practices obtained through the established information  
45 sharing network of local, state, federal and industry partners in which response team members  
46 regularly participate.

47 (e) The response team shall develop and maintain an updated cybersecurity incident  
48 response plan for the commonwealth and submit such plan annually for review, not later than  
49 November 1, to the governor and the joint committee on advanced information technology, the  
50 internet and cybersecurity. Said plan, which shall not be a public record pursuant to section 66,  
51 shall include, but not be limited to:

52 (i) ongoing and anticipated cybersecurity incidents or cybersecurity threats;

53 (ii) a risk analysis identifying the vulnerabilities of critical infrastructure and detailing  
54 risk-informed recommendations to address such vulnerabilities;

55 (iii) recommendations regarding the deployment of state agency resources and security  
56 professionals in rapidly responding to such cybersecurity incidents or cybersecurity threats; and

57 (iv) recommendations regarding best practices to minimize the impact of significant  
58 cybersecurity threats to agencies.

59 (f) In the event of a cybersecurity incident that threatens or results in a material  
60 impairment of the infrastructure or services of a state agency, the secretary of the executive  
61 office of technology services and security shall, with the approval of the governor, serve as the  
62 director of the response team; provided, however, that the secretary of the executive office of  
63 technology services and security may direct the response team to collaborate with other state  
64 agencies and entities that are not members of the response team as appropriate to respond to a  
65 cybersecurity incident.

66 (g) State agencies shall comply with all protocols and procedures established by the  
67 response team and all related policies, standards and administrative directives issued by the  
68 executive office of technology services and security pursuant to subsection (b) of section 3 of  
69 this chapter. The chief information officer or equivalent responsible officer for any state agency  
70 served by the executive office of technology services and security shall, as soon as practicable,  
71 report any known cybersecurity incident to the commonwealth security operations center, in a  
72 form to be prescribed by the executive office of technology services and security. The  
73 commonwealth security operations center shall notify the response team of all reported security  
74 threats or incidents as soon as practicable, but no later than 24 hours after receiving a report.

75 (h) The commonwealth fusion center and the commonwealth security operations center  
76 shall routinely exchange information related to cybersecurity threats and cybersecurity incidents  
77 that have been reported to or discovered by their respective state agencies or reported to the  
78 response team.

79 (i) The executive office of technology services and security and the response team shall  
80 consult with the Massachusetts Cyber Center and assist said center with efforts to foster  
81 cybersecurity resiliency through communications, collaboration and outreach to state agencies,  
82 municipalities, educational institutions and industry partners.

83 (j) Notwithstanding anything in this section to the contrary, other agencies not served by  
84 the executive office of technology services may report cybersecurity threats or cybersecurity  
85 incidents to the commonwealth security operations center in a form to be prescribed by the  
86 executive office of technology services and security.

87 (k) All employees of the executive agencies of the commonwealth shall be required to  
88 annually complete a security awareness training program approved by the executive office of  
89 technology services and security and administered by the human resources division.

90 (l) The secretary of the executive office of technology services and security shall  
91 promulgate regulations or directives to carry out the purposes of this section.

## 92 Section 13. Municipal and Critical Infrastructure Cyber Incident Reporting Requirements

93 (a) As used in this section, the following words shall have the following meanings unless  
94 the context clearly requires otherwise:

95 “Covered entity”, any (i) agency, office, department, board, commission, bureau, division  
96 or authority of a municipality or any political subdivision thereof; or (ii) an entity that owns or  
97 operates critical infrastructure.

98 “Secretary”, the secretary of the executive office of public safety and security.

99 (b) A covered entity shall provide notice, as soon as practicable and without unreasonable  
100 delay when such covered entity knows or has reason to know of a cybersecurity incident to the  
101 commonwealth fusion center in a form to be prescribed by the secretary in consultation with the  
102 response team; provided, however, that such notice shall include, but not be limited to:

103 (i) a timeline of events as best known by the covered entity and the type of cybersecurity  
104 incident known or suspected;

105 (ii) how the cybersecurity incident was initially detected or discovered;

106 (iii) a list of the specific assets that have been affected or are suspected to be affected;

107 (iv) copies of any electronic communications that are suspected of being malicious, if  
108 applicable;

109 (v) copies of any malware, threat actor tool or malicious links suspected of causing the  
110 cybersecurity incident, if applicable;

111 (vi) any digital logs such as firewall, active directory and event logs, if available;

112 (vii) forensic images of random access memory or virtualized random access memory  
113 from affected systems, if available;

114 (viii) contact information for the covered entity and any third-party entity engaging in  
115 cybersecurity incident response that is involved; and

116 (ix) any other information as required by the commonwealth fusion center or secretary.

117 (c) Upon receipt of said notice, the representative of the commonwealth fusion center to  
118 the response team or their designee shall:

119 (i) create and maintain a record of the cybersecurity incident, including all information  
120 provided by the covered entity in the notice under subsection (b);

121 (ii) provide a copy of said record to the response team to be included in the response  
122 team's annual cyber incident response plan required by subsection (e) of section 12; provided,  
123 however, that such copy shall not include any information identifiable to the covered entity that  
124 is not expressly necessary for the preparation of the response team's report unless the covered  
125 entity has provided affirmative consent to share such information; and

126 (iii) if the covered entity is a municipality or municipal agency under clause (i) of the  
127 definition of covered entity in this section, provide notice of the cybersecurity incident to the  
128 appropriate local law enforcement agency, including the contact information of the covered  
129 entity; provided, however, that this notification shall not be construed to fulfill any of the  
130 covered entity's reporting obligations under this chapter.

131 (d) Upon receipt of the notice required by subsection (b), the commonwealth fusion  
132 center may:



133 (i) coordinate with the response team to identify or communicate recommended response  
134 measures as appropriate; provided, however, that such recommended response measures shall  
135 not include the payment of a ransom;

136 (ii) assist the covered entity with implementing recommended response measures as  
137 appropriate, alone or in conjunction with: (1) any agency or entity represented in the response  
138 team; (2) any local law enforcement agency; or (3) the Massachusetts Cyber Center; and

139 (iii) provide, at the discretion of the secretary, information about other entities that are  
140 capable of providing mitigation and remediation support following a cybersecurity incident or in  
141 response to a cybersecurity threat.

142 (e) Nothing in this section shall be construed to:

143 (i) fulfill any regulatory data breach reporting requirements pursuant to chapter 93H; or

144 (ii) absolve any duty under applicable federal law to report a cybersecurity threat or  
145 cybersecurity incident to the cybersecurity and infrastructure security agency.

146 (f) This section shall not apply to a covered entity pursuant to clause (ii) of the definition  
147 of a covered entity that reports the cybersecurity incident to the cybersecurity and infrastructure  
148 security agency pursuant to the federal Cyber Incident Reporting for Critical Infrastructure Act  
149 of 2022 and its implementing regulations.

150 (g) The secretary, alone or in conjunction with the secretary of the executive office of  
151 technology services and security, shall promulgate regulations for the purposes of carrying out  
152 this section.

153           SECTION 2. Section 12 of chapter 7D of the General Laws, as inserted by section 1 of  
154 this act, shall take effect upon the passage of this act.

155           SECTION 3. Section 13 of chapter 7D of the General Laws, as inserted by section 1 of  
156 this act, shall take effect 12 months after the passage of this act.