SENATE DOCKET, NO. 2404 FILED ON: 1/20/2023

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:	DISTRICT/ADDRESS:
Barry R. Finegold	*Second Essex and Middlesex*

SENATE DOCKET, NO. 2404 FILED ON: 1/20/2023

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:

SECTION 1. Chapter 7D of the General Laws, as appearing in the 2022 Official Edition, is hereby amended by inserting after section 11 the following new sections:-

Section 12. State-Level Incident Reporting and Response

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

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

"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.

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

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

"Response team", the Massachusetts Cyber Incident Response Team established pursuant to this section.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 13. Municipal and Critical Infrastructure Cyber Incident Reporting Requirements

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

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

"Secretary", the secretary of the executive office of public safety and security.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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