SENATE . . . . . No. 2811

Senate, June 6, 2024 -- Text of amendment (19) (offered by Senator Moore) to the Ways and Means amendment (Senate, No. 2806) to the Senate Bill to provide for the future information technology needs of Massachusetts

The Commonwealth of Massachusetts

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

by inserting after section __ the following section:-

"SECTION __. Chapter 7D of the general laws is hereby amended by inserting at the end there of the following new sections:-

Section 13. Definitions.

As used in this section, and sections 14 through 16, inclusive, the following words shall have the following meanings, unless the context clearly requires otherwise:

“Artificial intelligence”, shall mean a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to: (1) perceive real and virtual environments; (2) abstract such perceptions into models through analysis in an automated manner; and (3) use model inference to formulate options for information or action.

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

“Covered Entity", shall mean (i) any governmental entity; or (ii) any entity operating or conducting business within the Commonwealth, but shall not include a small business.

“Critical infrastructure”, the assets, systems, and networks, 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, and shall include any critical infrastructure sectors as identified by (1) the by Presidential Policy Directive-21 or successor directive; the Cybersecurity and Infrastructure Security Agency; or (3) the cybersecurity control board.

“Cybersecurity incident”, an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of this definition, a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

“Cybersecurity threat”, Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, denial of service, or any combination thereof.

"Cybersecurity threat" shall also include the potential for a threat-source to successfully exploit a particular information system vulnerability..

"Governmental Entity", any department of state, county or local government including the executive, legislative or judicial, and all councils thereof and thereunder, and any division, board, bureau, commission, institution, tribunal or other instrumentality within such department, and any independent state, county or local authority, district, commission, instrumentality or agency.

"Government-Issued Device", shall include cell phones, desktop computers, tablets, laptops, or any other device capable of connecting to the internet that is provided by or on behalf of a Governmental entity.

"Response team", the Massachusetts Cyber Incident Response Team, established pursuant to section 15.

"Small Business", any entity that based on: (i) its size and scope; (ii) the type of entity; (iii) the amount of resources available to such entity; and (iv) the amount and type of stored data and the need for security and confidentiality of said data; that said entity does not face a reasonable risk of encountering a cybersecurity incident, provided that a "small business" shall not include: (i) any entity which has operations or business related to critical infrastructure, either in whole or part; or (ii) any governmental entity. The cybersecurity control board shall further define the term "Small Business" pursuant to section 14(a)(i)(1)(F) of this chapter.

Section 14. Cybersecurity Control Board.

(a) There is hereby established within the executive office of technology services and security a board, to be known as the cybersecurity control board, responsible for adopting and administering a state cybersecurity code.

(i) The board shall have the following powers and duties:

(1) To formulate, propose, adopt and amend rules and regulations, pursuant to chapter 30A, relating to:

(A) minimum cybersecurity standards or requirements for covered entities, including but not limited to, standards and requirements related to:

(i) user authentication and permissions;

(ii) asset and data governance, minimization, mapping, management, classification, transfer, storage, retention, and responsible end-of-life, including but not limited to,, destruction, deletion, or safeguarding;

(iii) cybersecurity training;

(iv) device issuance and management;

(v) system and network design, security and monitoring;

(vi) encryption;

(vii) artificial intelligence;

(viii) physical access to systems;

(ix) vulnerability patching and threat mitigation;

(x) auditing and testing, including but not limited to, penetration testing, access control reviews, and physical security assessments; and

(xi) any other cybersecurity standards or requirements that would materially decrease the risk of a cybersecurity incident.

(B) special cybersecurity standards for subsets of covered entities based on industry, size, type of entity, or any combination thereof, including but not limited to:

(i) critical infrastructure; and

(ii) entities that contract with or store, distribute, transfer, process, or manage data on behalf of a governmental entity.

(C) the creation by covered entities of cybersecurity policies, incident response plans, table-top exercises, and other steps required to update such policies and plans in light of evolving risk;

(D) the creation and administration of a cybersecurity accreditation or certification program to ensure compliance by covered entities with the requirements of the state cybersecurity code, and recognition for covered entities that exceed the requirements of the state cybersecurity code, including the selection of certain qualified third-party entities to implement said accreditation or certification program;

(E) identify critical infrastructure sectors;

(F) further define the term “Small Business”; and

(G) the issuance and enforcement of any penalties for violation of the state cybersecurity code by a covered entity.

(H) Such rules and regulations shall take into account, with regard to covered entities:

(i) their size and scope;

(ii) type of entity, including whether the entity is part of local government;

(iii) the amount of resources available to a covered entity;

(iv) the amount and type of stored data and the need for security and confidentiality of such data; and

(v) any other factors deemed appropriate by the board.

(I) Such rules and regulations, together with any penalties for the violation thereof, as hereinafter provided, shall comprise and be collectively known as the state cybersecurity code.

Whoever violates any provision of the state cybersecurity code shall be punished by a fine of not more than ten thousand dollars. Each day during which a violation exists shall constitute a separate offense.

For each violation of the state cybersecurity code, the board may permit, and qualify or condition, a cure period for said violation, provided that any decision to set a cure period shall take into consideration:

(1) the nature of the violation;

(2) the potential or actual harm from the violation;

(3) efforts made by the covered entity to prevent or remedy the violation;

(4) the number and nature of previous violations by the covered entity; and

(5) any other aggravating factors or mitigating circumstances deemed appropriate by the board.

(J) Such rules and regulations shall be guided by National Institute of Standards and Technology standards, the Cybersecurity and Infrastructure Security Agency cybersecurity performance goals and other applicable federal guidance, and shall be consistent with chapters 93H and 93I.

(K) The board shall revise and amend the state cybersecurity code at least once every five years.

(2) To subpoena witnesses, take testimony, compel production of books and records and to hold public hearings. The board may designate one or more of its members to hold special public hearings and report on such hearings to the board.

(3) To make a continuing study of the operation of the state cybersecurity code, and other laws and regulations relating to cybersecurity, provided the cybersecurity control board shall issue recommendations for legislative changes related to cybersecurity to the governor, the house and senate committees on ways and means and the joint committee on advanced information technology, the internet and cybersecurity.

(4) To formulate administrative procedures and promulgate rules and regulations, pursuant to chapter 30A, necessary to administer and enforce this section, establish the Cyber

Incident Response Team under section 15, and the critical infrastructure reporting requirements under section 16.

(5) To coordinate with federal agencies and utilize federal resources and services.

(6) To issue, amend or revoke critical cybersecurity directives to protect government issued systems and devices from substantial cybersecurity risks, notwithstanding any general or special law to the contrary, provided:

(A) Directives may prohibit, limit, condition or qualify, the installation or use of any hardware, software, system, supply or service by government-issued systems or devices; and may establish related restrictions on non-government issued devices or systems that connect with government-issued systems or devices;

(B) Directives shall specify a reasonable time frame for the directive's implementation, provided the board may require immediate implementation;

(C) Directives shall be effective upon transmittal to any applicable governmental entity;

(D) Any governmental entity which receives a directive shall implement such directive consistent with the terms and time frame of said directive and shall certify, in writing, to the board upon both the receipt and final implementation of said directive; provided that a governmental entity may apply to the board for relief from, or modification of, said directive as provided hereinafter; and

(E) Upon application to the board by a government entity, or on the board's own initiative, the board may waive, delay or suspend implementation of any directive, or any part or parts thereof, applicable to said government entity and, in the board's discretion, other similarly

situated government entities, provided that the board shall determine in writing that such waiver, delay, or suspension shall not substantially increase the risk of a cybersecurity incident.

(F) Chapter 30A shall not apply to critical cybersecurity directives.

(b) (i)The board shall consist of the following members: the secretary of the executive office of technology services and security, or their designee, who shall serve as chair; the secretary of the executive office of public safety and security, or their designee; the comptroller or their designee; the adjunct general of the national guard or their designee; the colonel of the state police or their designee; the executive director of the Massachusetts Technology Collaborative or their designee; the director of Legislative Information Services, or their designee; the director of Judicial Information Services Department, or their designee; one member appointed by the Massachusetts CyberTrust; the Attorney General, or their designee; one member appointed by the Massachusetts Municipal Association; 9 members of the public appointed by the Governor who shall have experience related to cybersecurity; provided each shall have at least 5 years of experience related to cybersecurity in the following fields, respectively: finance; healthcare; technology services; utilities; transportation services; academia or cryptography; operational technologies ; law enforcement or homeland security; and experience with cybersecurity on the federal level.

(ii) Public members of the board shall serve without compensation. Public members of the board shall be reimbursed for all necessary expenses incurred in the discharge of their official duties.

(iii) A majority of the members of the board shall constitute a quorum for the purpose of conducting business, but a lesser number may adjourn from time to time. The board shall keep

detailed and accurate minutes of its meetings and shall publish such minutes within 30 days of each meeting.

(iv) Each member shall be appointed for a term of five years and shall be eligible for reappointment; provided, however, that no public member shall serve more than 10 years. Any person appointed to fill a vacancy shall serve only for the unexpired term. Any public member of the board may be removed by the governor for cause, after being given a written statement of the charges and an opportunity to be heard thereon. No member shall act as a member of the board or vote in connection with any matter as to which their private right, distinct from public interest, is concerned.

(v) The chair shall have and exercise supervision and control over all the affairs of the board. The chair shall preside at all meetings at which the chair is present and shall designate a member of the board to act as chair in the chair's absence. To promote efficiency in administration, the chair shall make such division or re-division of the work of the board among the members of the board as the chair deems expedient and may divide and re-divide the board into subcommittees.

(vi) The board shall meet not less than four times in a calendar year.

(vii) The board's activities shall be supported by staff of the secretary of the executive office of technology services and security.

(c) The board or the attorney general may issue and recover penalties and enforce the provisions of sections 13 through 16, inclusive. The attorney general may enforce these sections pursuant to section 4 of chapter 93A.

Section 15. Massachusetts Cyber Incident Response Team.

(a) There shall be established a Massachusetts Cyber Incident Response Team, which shall serve as a standing subcommittee of the cybersecurity control board established under section 14, the mission of which is to enhance this commonwealth's ability to prepare for, respond to, mitigate against and recover from significant cybersecurity incidents.

(b) The response team shall consist of: the secretary of the executive office of technology services and security or their designee, who shall serve as chair of the response team; a representative of the commonwealth security operations center as designated by the director of security operations; the secretary of the executive office of public safety and security or their designee; a representative of the state police cyber crime unit; a representative of the commonwealth fusion center; the adjutant general of the Massachusetts National Guard or their designee; the director of the Massachusetts emergency management agency or their designee; the comptroller or their designee; and any other state or local officials or members of the cybersecurity control board as assigned by the chair. The chair shall designate a member of the response team to act as a liaison with federal agencies.

(c) The response team shall review cybersecurity threat information (including intrusion methods, common techniques, and known vulnerabilities) to make informed recommendations and establish appropriate policies to manage the risk of cybersecurity incidents for all governmental entities; 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.

(d) 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. The response team shall conduct tabletop exercises to test the plan at least twice per year and shall conduct individual tabletop exercise testing with a subset of governmental entities , as selected by the response team, at least quarterly. Said plan, which shall not be a public record pursuant to chapter 66 or clause twenty six of section 7 of chapter 4, 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 governmental entity resources and security professionals in rapidly responding to such cybersecurity incidents or cybersecurity threats;

(iv) recommendations regarding best practices to minimize the impact of significant cybersecurity threats to governmental entities; and

(v) guidelines for governmental entities regarding communication with an individual or entity that is demanding a payment of ransom related to a cybersecurity incident

(e) In the event of a cybersecurity incident that threatens or results in a material impairment of the infrastructure or services of a governmental entity or critical infrastructure, 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 governmental entities, including federal entities, that are not members of the response team as appropriate to respond to a cybersecurity incident. The provisions of the open meeting law, sections 18 through 25, inclusive, of chapter 30A, shall not apply to meetings, communications, deliberations or other activities of the Critical Incident Response Team conducted in response to a cybersecurity incident under this subsection.

(f) Governmental entities 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 governmental entity shall, as soon as practicable, report any known cybersecurity incident as soon as practicable 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.

(g) The commonwealth fusion center and the commonwealth security operations center shall routinely exchange information with the response team and CISA 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.

(h) 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 governmental entities, educational institutions and industry partners.

(i) The cybersecurity control board shall promulgate regulations or directives to carry out the purposes of this section.

Section 16. 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 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 related to the cybersecurity incident as required by the secretary.

Any notice provided by a covered entity under this subsection shall not be a public record pursuant to chapter 66 or clause twenty six of section 7 of chapter 4.

(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); and

(ii) provide a copy of said record to the response team, which will be included in the Response Team's annual cyber incident response plan required by subsection (d) of section 15; 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.

(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;

(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; (3) private individuals and other entities at the discretion of the secretary; or (4) 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 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, in consultation with the secretary of the executive office of technology services and security, shall promulgate regulations for the purposes of carrying out this section.