

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

---

**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 relative to cybersecurity and artificial intelligence.**

\_\_\_\_\_

PETITION OF:

NAME:

*Michael O. Moore*

DISTRICT/ADDRESS:

*Second Worcester*

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

---

---

[Pin Slip]

---

---

[SIMILAR MATTER FILED IN PREVIOUS SESSION  
SEE SENATE, NO. 2539 OF 2023-2024.]

**The Commonwealth of Massachusetts**

\_\_\_\_\_  
**In the One Hundred and Ninety-Fourth General Court  
(2025-2026)**  
\_\_\_\_\_

An Act relative to cybersecurity and artificial intelligence.

*Whereas*, The deferred operation of this act would tend to defeat its purpose, which is to further regulate cybersecurity and artificial intelligence, therefore it is hereby declared to be an emergency law, necessary for the immediate preservation of the public safety.

*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 is hereby amended by inserting at the end  
2 there of the following new sections:-

3 Section 12. Statewide Public Employee Cybersecurity Training.

4 (a) Every state, county, and municipal employee shall, within 30 days after becoming  
5 such an employee, and every year thereafter, complete general cybersecurity awareness training.  
6 Each state, county, and municipal agency shall establish policies requiring such training and  
7 upon completion of the training program the employee shall provide notice of such completion to  
8 be retained for 6 years by the appropriate employer.

9 (b) The executive office of technology services and security, in consultation with the  
10 office of the comptroller, shall prepare and update from time to time the following online  
11 training programs, which the executive office shall publish or make available on its official  
12 website: (1) a program which shall provide general cybersecurity awareness training; and (2)  
13 special programs, which may be tailored to an agency, profession, role, cybersecurity threat, or  
14 other factors that said executive office determines is necessary to enhance cybersecurity within  
15 the commonwealth. The executive office shall consult benchmarks and standards established by  
16 the Center for Internet Security, National Institute for Standards and Technology and the  
17 Workforce Framework for Cybersecurity in developing the cybersecurity trainings.

18 (c) Completion of the general cybersecurity awareness training provided under subsection  
19 (b)(1) by a state, county, or municipal employee shall satisfy the general cybersecurity training  
20 requirement of subsection (a).

21 (d) In lieu of the general cybersecurity awareness training provided under subsection  
22 (b)(1), a state, county, or municipal agency may satisfy the general cybersecurity awareness  
23 training requirement of subsection (a) by requiring their employees to complete general  
24 cybersecurity awareness training provided or made available by said agency.

25 (e) A state, county, or municipal agency may establish policies requiring additional,  
26 special or supplemental cybersecurity trainings for their employees.

27 (f) For the purposes of this section, the terms state, county, and municipal employee, and  
28 state, county, and municipal agency shall have the same meanings as defined by section 1 of  
29 chapter 268A.

30 Section 13. Definitions.

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

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

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

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

42 “Critical infrastructure”, the assets, systems, and networks, either physical or virtual,  
43 within the commonwealth that are so vital to the commonwealth or the United States that the  
44 incapacitation or destruction of such a system or asset would have a debilitating impact on  
45 physical security, economic security, public health or safety or any combination thereof;  
46 provided, however, that “critical infrastructure” shall include, but not be limited to, election  
47 systems, transportation infrastructure, water, gas and electric utilities, and shall include any  
48 critical infrastructure sectors as identified by (1) the by Presidential Policy Directive-21 or  
49 successor directive; the Cybersecurity and Infrastructure Security Agency; or (3) the  
50 cybersecurity control board.

51 “Cybersecurity incident”, an event occurring on or conducted through a computer  
52 network that actually or imminently jeopardizes the integrity, confidentiality, or availability of

53 computers, information or communications systems or networks, physical or virtual  
54 infrastructure controlled by computers or information systems, or information resident thereon.  
55 For purposes of this definition, a cyber incident may include a vulnerability in an information  
56 system, system security procedures, internal controls, or implementation that could be exploited  
57 by a threat source.

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

62 “Cybersecurity threat” shall also include the potential for a threat-source to successfully exploit a  
63 particular information system vulnerability..

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

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

72 “Response team”, the Massachusetts Cyber Incident Response Team, established  
73 pursuant to section 15.

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

81 Section 14. Cybersecurity Control Board.

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

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

86 (1) To formulate, propose, adopt and amend rules and regulations, pursuant to chapter  
87 30A, relating to:

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

90 (i) user authentication and permissions;

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

94 (iii) cybersecurity training;

- 95 (iv) device issuance and management;
- 96 (v) system and network design, security and monitoring;
- 97 (vi) encryption;
- 98 (vii) artificial intelligence;
- 99 (viii) physical access to systems;
- 100 (ix) vulnerability patching and threat mitigation;
- 101 (x) auditing and testing, including but not limited to, penetration testing, access control  
102 reviews, and physical security assessments; and
- 103 (xi) any other cybersecurity standards or requirements that would materially decrease the  
104 risk of a cybersecurity incident.
- 105 (B) special cybersecurity standards for subsets of covered entities based on industry, size,  
106 type of entity, or any combination thereof, including but not limited to:
- 107 (i) critical infrastructure; and
- 108 (ii) entities that contract with or store, distribute, transfer, process, or manage data on  
109 behalf of a governmental entity.
- 110 (C) the creation by covered entities of cybersecurity policies, incident response plans,  
111 table-top exercises, and other steps required to update such policies and plans in light of evolving  
112 risk;

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

118 (E) identify critical infrastructure sectors;

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

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

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

123 (i) their size and scope;

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

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

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

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

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



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

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

137           (1) the nature of the violation;

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

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

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

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

143           (J) Such rules and regulations shall be guided by National Institute of Standards and  
144 Technology standards, the Cybersecurity and Infrastructure Security Agency cybersecurity  
145 performance goals and other applicable federal guidance, and shall be consistent with chapters  
146 93H and 93I.

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

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

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

157           (4) To formulate administrative procedures and promulgate rules and regulations,  
158 pursuant to chapter 30A, necessary to administer and enforce this section, establish the Critical  
159 Incident Response Team under section 15, and the critical infrastructure reporting requirements  
160 under section 16.

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

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

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

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

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

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

177 (E) Upon application to the board by a government entity, or on the board's own  
178 initiative, the board may waive, delay or suspend implementation of any directive, or any part or  
179 parts thereof, applicable to said government entity and, in the board's discretion, other similarly  
180 situated government entities, provided that the board shall determine in writing that such waiver,  
181 delay, or suspension shall not substantially increase the risk of a cybersecurity incident.

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

183 (b) (i) The board shall consist of the following members: the secretary of the executive  
184 office of technology services and security, or their designee, who shall serve as chair; the  
185 secretary of the executive office of public safety and security, or their designee; the comptroller  
186 or their designee; the adjunct general of the national guard or their designee; the colonel of the  
187 state police or their designee; the executive director of the Massachusetts Technology  
188 Collaborative or their designee; the director of Legislative Information Services, or their  
189 designee; the director of Judicial Information Services Department, or their designee; one  
190 member appointed by the Massachusetts CyberTrust; the Attorney General, or their designee;

191 one member appointed by the Massachusetts Municipal Association; 9 members of the public  
192 appointed by the Governor who shall have experience related to cybersecurity; provided each  
193 shall have at least 5 years of experience related to cybersecurity in the following fields,  
194 respectively: finance; healthcare; technology services; utilities; transportation services; academia  
195 or cryptography; operational technologies ; law enforcement or homeland security; and  
196 experience with cybersecurity on the federal level.

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

200 (iii) A majority of the members of the board shall constitute a quorum for the purpose of  
201 conducting business, but a lesser number may adjourn from time to time. The board shall keep  
202 detailed and accurate minutes of its meetings and shall publish such minutes within 30 days of  
203 each meeting.

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

211 (v) The chair shall have and exercise supervision and control over all the affairs of the  
212 board. The chair shall preside at all meetings at which the chair is present and shall designate a

213 member of the board to act as chair in the chair's absence. To promote efficiency in  
214 administration, the chair shall make such division or re-division of the work of the board among  
215 the members of the board as the chair deems expedient and may divide and re-divide the board  
216 into subcommittees.

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

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

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

223 Section 15. Massachusetts Cyber Incident Response Team.

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

228 (b) The response team shall consist of: the secretary of the executive office of technology  
229 services and security or their designee, who shall serve as chair of the response team; a  
230 representative of the commonwealth security operations center as designated by the director of  
231 security operations; the secretary of the executive office of public safety and security or their  
232 designee; a representative of the state police cyber crime unit; a representative of the  
233 commonwealth fusion center; the adjutant general of the Massachusetts National Guard or their

234 designee; the director of the Massachusetts emergency management agency or their designee; the  
235 comptroller or their designee; and any other state or local officials or members of the  
236 cybersecurity control board as assigned by the chair. The chair shall designate a member of the  
237 response team to act as a liaison with federal agencies.

238 (c) The response team shall review cybersecurity threat information (including intrusion  
239 methods, common techniques, and known vulnerabilities) to make informed recommendations  
240 and establish appropriate policies to manage the risk of cybersecurity incidents for all  
241 governmental entities; provided, however, that such recommendations, policies and directives  
242 shall be informed by information and best practices obtained through the established information  
243 sharing network of local, state, federal and industry partners in which response team members  
244 regularly participate.

245 (d) The response team shall develop and maintain an updated cybersecurity incident  
246 response plan for the commonwealth and submit such plan annually for review, not later than  
247 November 1, to the governor and the joint committee on advanced information technology, the  
248 internet and cybersecurity. The response team shall conduct tabletop exercises to test the plan at  
249 least twice per year and shall conduct individual tabletop exercise testing with a subset of  
250 governmental entities, as selected by the response team, at least quarterly. Said plan, which shall  
251 not be a public record pursuant to chapter 66 or clause twenty six of section 7 of chapter 4, shall  
252 include, but not be limited to:

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

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

256 (iii) recommendations regarding the deployment of governmental entity resources and  
257 security professionals in rapidly responding to such cybersecurity incidents or cybersecurity  
258 threats;

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

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

263 (e) In the event of a cybersecurity incident that threatens or results in a material  
264 impairment of the infrastructure or services of a governmental entity or critical infrastructure, the  
265 secretary of the executive office of technology services and security shall, with the approval of  
266 the governor, serve as the director of the response team; provided, however, that the secretary of  
267 the executive office of technology services and security may direct the response team to  
268 collaborate with other governmental entities, including federal entities, that are not members of  
269 the response team as appropriate to respond to a cybersecurity incident. The provisions of the  
270 open meeting law, sections 18 through 25, inclusive, of chapter 30A, shall not apply to meetings,  
271 communications, deliberations or other activities of the Critical Incident Response Team  
272 conducted in response to a cybersecurity incident under this subsection.

273 (f) Governmental entities shall comply with all protocols and procedures established by  
274 the response team and all related policies, standards and administrative directives issued by the  
275 executive office of technology services and security pursuant to subsection (b) of section 3 of  
276 this chapter. The chief information officer or equivalent responsible officer for any governmental  
277 entity shall, as soon as practicable, report any known cybersecurity incident as soon as

278 practicable to the commonwealth security operations center, in a form to be prescribed by the  
279 executive office of technology services and security. The commonwealth security operations  
280 center shall notify the response team of all reported security threats or incidents as soon as  
281 practicable, but no later than 24 hours after receiving a report.

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

286 (h) The executive office of technology services and security and the response team shall  
287 consult with the Massachusetts Cyber Center and assist said center with efforts to foster  
288 cybersecurity resiliency through communications, collaboration and outreach to governmental  
289 entities, educational institutions and industry partners.

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

292 Section 16. Critical Infrastructure Cyber Incident Reporting Requirements.

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

295 “Covered entity”, any entity that owns or operates critical infrastructure.

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

297 (b) A covered entity shall provide notice, as soon as practicable and without unreasonable  
298 delay when such covered entity knows or has reason to know of a cybersecurity incident to the



299 commonwealth fusion center in a form to be prescribed by the secretary in consultation with the  
300 Response Team; provided, however, that such notice shall include, but not be limited to:

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

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

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

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

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

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

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

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

314 (ix) any other information related to the cybersecurity incident as required by the  
315 secretary.

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

318 (c) Upon receipt of said notice, the representative of the commonwealth fusion center to  
319 the Response Team or their designee shall:

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

322 (ii) provide a copy of said record to the response team, which will be included in the  
323 Response Team's annual cyber incident response plan required by subsection (d) of section 15;  
324 provided, however, that such copy shall not include any information identifiable to the covered  
325 entity that is not expressly necessary for the preparation of the Response Team's report unless  
326 the covered entity has provided affirmative consent to share such information.

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

329 (i) coordinate with the Response Team to identify or communicate recommended  
330 response measures as appropriate;

331 (ii) assist the covered entity with implementing recommended response measures as  
332 appropriate, alone or in conjunction with: (1) any agency or entity represented in the Response  
333 Team; (2) any local law enforcement agency; (3) private individuals and other entities at the  
334 discretion of the secretary; or (4) the Massachusetts Cyber Center; and

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

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

339 (i) fulfill any regulatory data breach reporting requirements pursuant to chapter 93H; or  
340 (ii) absolve any duty under applicable federal law to report a cybersecurity threat or  
341 cybersecurity incident to the Cybersecurity and Infrastructure Security Agency.

342 (f) This section shall not apply to a covered entity that reports the cybersecurity incident  
343 to the Cybersecurity and Infrastructure Security Agency pursuant to the federal Cyber Incident  
344 Reporting for Critical Infrastructure Act of 2022 and its implementing regulations.

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

347 Section 17. Automated Decision Making Control Board.

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

350 “Algorithm”, a specific procedure, set of rules, or order of operations designed to solve a  
351 problem or make a calculation, classification, or recommendation.

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

358 “Automated decision system”, any computer program, method, statistical model, or  
359 process that aims to aid or replace human decision-making using algorithms or artificial

360 intelligence. These systems can include, but are not limited to, analyzing complex datasets about  
361 human populations and government services or other activities to generate scores, predictions,  
362 warnings, classifications, or recommendations.

363 “Commonwealth of Massachusetts” or “governmental unit”, any state, county, or  
364 municipal agency as defined by section 1 of chapter 268A.

365 “Covered Entity” means (1) any governmental unit; or (2) any entity within the  
366 commonwealth that utilizes an automated decision system.

367 “Identified group characteristic”, age, race, creed, color, religion, national origin, sex,  
368 gender identity, disability, sexual orientation, genetic information, marital status, pregnancy or a  
369 condition related to said pregnancy, ancestry, veteran status, receipt of public assistance,  
370 economic status, location of residence, or citizenship status.

371 “Source code”, the foundational programming of a computer application, model, or  
372 system that can be read and understood by people.

373 “Training data”, the data used to inform the development of an automated decision  
374 system and the decisions or recommendations it generates.

375 (b) There shall be a board within the executive office of technology services and security  
376 for the purpose of studying and making recommendations relative to the use of automated  
377 decision systems by covered entities within the Commonwealth that may affect human welfare,  
378 including, but not limited to, the legal rights and privileges of individuals. The board shall  
379 evaluate the use of automated-decision systems in the commonwealth, including government

380 use, and shall promulgate appropriate regulations, limits, standards and safeguards. The board  
381 shall:

382 (i) undertake a complete and specific survey of all uses of automated decision systems by  
383 covered entities and the purposes for which such systems are used, including but not limited to:

384 (1) the principles, policies, and guidelines adopted by covered entities to inform the  
385 procurement, evaluation, and use of automated decision systems, and the procedures by which  
386 such principles, policies, and guidelines are adopted;

387 (2) the training specific covered entities provide to individuals using automated decision  
388 systems, and the procedures for auditing and enforcing the principles, policies, and guidelines  
389 regarding their use;

390 (3) the manner by which covered entities validate and test the automated decision  
391 systems they use, and the manner by which they evaluate those systems on an ongoing basis,  
392 specifying the training data, input data, systems analysis, studies, vendor or community  
393 engagement, third-parties, or other methods used in such validation, testing, and evaluation;

394 (4) matters related to the transparency, explicability, auditability, and accountability of  
395 automated decision systems in use in covered entities, including information about their  
396 structure; the processes guiding their procurement, implementation and review; whether they can  
397 be audited externally and independently; and the people who operate such systems and the  
398 training they receive;

399 (5) the manner and extent to which covered entities make the automated decision systems  
400 they use available to external review, and any existing policies, laws, procedures, or guidelines

401 that may limit external access to data or technical information that is necessary for audits,  
402 evaluation, or validation of such systems;

403 (6) procedures and policies in place to protect the due process rights of individuals  
404 directly affected by Massachusetts offices' use of automated decision systems, including but not  
405 limited to public disclosure and transparency procedures; and

406 (7) the manner in which automated decision systems are assessed by covered entities,  
407 vendors or third parties for biases, including but not limited to, discrimination on the basis of  
408 identified group characteristics;

409 (ii) consult with experts in the fields of artificial intelligence, machine learning,  
410 algorithmic or artificial intelligence bias, algorithmic or artificial intelligence auditing, and civil  
411 and human rights;

412 (iii) examine research related to the use of automated decision systems that directly or  
413 indirectly result in disparate outcomes for individuals or communities based on an identified  
414 group characteristic;

415 (iv) conduct a survey of technical, legal, or policy controls to improve the just and  
416 equitable use of automated decision systems and mitigate any disparate impacts deriving from  
417 their use, including best practices, policy tools, laws, and regulations developed through research  
418 and academia or proposed or implemented in other states and jurisdictions;

419 (v) examine matters related to data sources, data sharing agreements, data security  
420 provisions, compliance with data protection laws and regulations, and all other issues related to

421 how data is protected, used, and shared by agencies using automated decision systems, in  
422 Massachusetts and in other jurisdictions;

423 (vi) examine matters related to automated decision systems and intellectual property,  
424 such as the existence of non-disclosure agreements, trade secrets claims, and other proprietary  
425 interests, and the impacts of intellectual property considerations on transparency, explicability,  
426 auditability, accountability, and due process; and

427 (vii) examine any other opportunities and risks associated with the use of automated  
428 decision systems by covered entities.

429 (c) The board shall consist of the secretary of technology services and security or the  
430 secretary's designee, who shall serve as chair; 1 member of the Senate, designated by the senate  
431 president; 1 member of the house of representatives, designated by the speaker of the house of  
432 representatives; the chief justice of the supreme judicial court or a designee; the secretaries of the  
433 Executive Office of Public Safety and Security, and Executive Office of Health and Human  
434 Services, or their designees; the executive director of the American Civil Liberties Union of  
435 Massachusetts or a designee; 3 representatives from academic institutions in the Commonwealth  
436 to be appointed by the Governor who shall be experts in (i) artificial intelligence and machine  
437 learning; (ii) data science and information policy; (iii) social implications of artificial intelligence  
438 and technology; or (iv) technology and the law; the executive director of the Massachusetts Law  
439 Reform Institute or a designee; 1 representative from the National Association of Social  
440 Workers; 1 representative from the NAACP; 1 representative from the Massachusetts  
441 Technology Collaborative; and 1 representative from the Massachusetts High Technology  
442 Council; and 6 representatives of the business community, to be appointed by the Governor, who

443 shall have relevant experience in at least two of the following fields: (i) artificial intelligence and  
444 machine learning; (ii) data science and information policy; (iii) social implications of artificial  
445 intelligence and technology; or (iv) technology and the law.

446 (d) Members of the board shall be appointed within 45 days of the effective date of this  
447 act and within 45 days of any vacancy. Any vacancy shall be filled in the same manner as the  
448 original appointment. The board shall meet at the call of the chair based on the board's workload  
449 but not fewer than 10 times per calendar year. The board shall hold at least one public hearing  
450 per year to solicit feedback from Massachusetts residents and other interested parties. The  
451 board's meetings shall be broadcast over the internet.

452 (e) The board shall submit an annual report by December 31 to the governor, the clerks of  
453 the house of representatives and the senate, and the joint committee on advanced information  
454 technology, the internet and cybersecurity. The report shall be a public record and it shall  
455 include, but not be limited to:

456 (i) a description of the board's activities and any community engagement undertaken by  
457 the board;

458 (ii) the board's findings, including but not limited to the publication of a list of all  
459 automated decision systems in use by governmental units, the policies, procedures, and training  
460 guidelines in place to govern their use, and any contracts with third parties pertaining to the  
461 acquisition or deployment of such systems.

462 (f) The board shall promulgate, amended, or rescind rules and regulations to establish  
463 standards and safeguards to:



464 (i) Promote racial and economic justice, equity, fairness, accountability, and transparency  
465 in the use of automated decision systems by covered entities;

466 (ii) Establish areas where governmental units shall not use automated decision systems or  
467 any qualifications, conditions, limits or prohibitions that shall be set on governmental use of an  
468 automated decision system;

469 (iii) Requirements for the adoption of policies and procedures by governmental units for  
470 the following purposes:

471 (1) to allow a person affected by a rule, policy, or action made by, or with the assistance  
472 of, an automated decision system, to request and receive an explanation of such rule, policy, or  
473 action and the basis therefor;

474 (2) to determine whether an automated decision system disproportionately or unfairly  
475 impacts a person or group based on an identified group characteristic;

476 (3) to determine prior to or during the procurement or acquisition process whether a  
477 proposed governmental unit automated decision system is likely to disproportionately or unfairly  
478 impact a person or group based on an identified group characteristic;

479 (4) to address instances in which a person or group is harmed by a governmental unit  
480 automated decision system if any such system is found to disproportionately impact a person or  
481 group on the basis of an identified group characteristic; and

482 (5) to make information publicly available that, for each automated decision system, will  
483 allow the public to meaningfully assess how such system functions and is used by a  
484 governmental unit, including making technical information about such system publicly available.

485 (iv) Regulate the training data related to an automated decision system, including but not  
486 limited to:

487 (1) security measures to protect that data of individuals used as part of the training data;

488 (2) informed consent, as defined by the board, from individuals before collecting, using,  
489 sharing or disclosing their data; and

490 (3) the deletion or de-identification of any data collected from individuals if it is no  
491 longer needed for the intended purpose of the training data or automated decision system.

492 (g) Whoever violates any provision of this section, and any regulations promulgated by  
493 the board, shall be punished by a fine of not more than one thousand dollars for each such  
494 violation. Each day during which a violation exists shall constitute a separate offense.

495 (f) The board or the attorney general may issue and recover penalties and enforce the  
496 provisions of this section. The attorney general may enforce this section pursuant to section 4 of  
497 chapter 93A.

498 SECTION 2. Chapter 23G of the general laws is hereby amended by inserting at the end  
499 thereof the following new section:-

500 Section 48. Massachusetts Innovation Fund and State Agency Technology Upgrades  
501 Account

502 (a) As used in this section, the following terms shall have the following meanings:-

503 "Account", the state agency technology upgrades account.

504 "Board", the Massachusetts innovation fund board.

505 "Cloud computing service", has the meaning given the term by the National Institute of  
506 Standards and Technology in NIST Special Publication 800-145 and any amendatory or  
507 superseding document thereto.

508 "Device-as-a-service", a managed service in which hardware that belongs to a managed  
509 service provider is installed at a state agency and a service level agreement defines the  
510 responsibilities of each party to the agreement.

511 "Fund", means the Massachusetts Innovation Fund.

512 "Information technology system", any equipment or interconnected system or subsystem  
513 of equipment used by a state agency, or a person under a contract with a state agency if the  
514 contract requires use of the equipment, to acquire, store, analyze, evaluate, manipulate, manage,  
515 move, control, display, switch, interchange, transmit, print, copy, scan, or receive data or other  
516 information. "Information technology system" shall include, but not be limited to, operational  
517 technology, including industrial control systems, a computer, a device-as-a-service solution,  
518 ancillary computer equipment such as imaging, printing, scanning, and copying peripherals and  
519 input, output, and storage devices necessary for security and surveillance, peripheral equipment  
520 designed to be controlled by the central processing unit of a computer, software and firmware  
521 and similar procedures, and services, including support services, and related resources.  
522 "Information technology system" shall not include equipment acquired by a contractor incidental  
523 to a state contract.

524 "Legacy information technology system", is an information technology system that is  
525 operated with outdated or obsolete, or inefficient hardware or software system of information  
526 technology.

527 "Qualifying information technology modernization project", a project by a state agency to  
528 (i) replace the agency's information technology systems; (ii) transition the agency's legacy  
529 information technology systems to a cloud computing service or other innovative commercial  
530 platform or technology; (iii) develop and implement a method to provide adequate, risk-based,  
531 and cost-effective information technology responses to threats to the agency's information  
532 security; (iv) reducing data, hardware, and software redundancy; (v) improving system and data  
533 interoperability; or (vi) implementing cybersecurity solutions consistent with principles of Zero  
534 Trust architecture as defined by the National Institute of Standards and Technology.

535 (b) The Massachusetts innovation fund board is established to administer the  
536 Massachusetts innovation fund and the state agency technology upgrades account and to make  
537 awards of financial assistance to state agencies from the fund or account for qualifying  
538 information technology modernization projects. The board shall consist of: (i) the executive  
539 director of Massachusetts Development Finance Agency or a designee; (ii) the secretary of the  
540 executive office of technology services and security or a designee; (iii) the governor or a  
541 designee; (iv) two members of the senate appointed by the president of the senate; (v) two  
542 members of the house of representatives appointed by the speaker of the house of  
543 representatives; (vi) one member of the public with relevant subject matter expertise appointed  
544 by the governor; and (vii) three state employees primarily having technical expertise in  
545 information technology development, financial management, cybersecurity and privacy, and  
546 acquisition, appointed by the secretary of the executive office of technology services and  
547 security.

548 (c) Members of the board shall serve up to six two-year terms. A board member is not  
549 entitled to compensation for service on the board but is entitled to reimbursement of expenses  
550 incurred while performing duties as a board member.

551 (d) The Massachusetts innovation fund and the state agency technology upgrades account  
552 are each established and set up on the books of the commonwealth as a separate fund, and may  
553 be expended from without further legislative appropriation, as provided by this section.  
554 MassDevelopment shall hold the Massachusetts innovation fund and the state agency technology  
555 upgrades account in separate accounts and apart from all other accounts.

556 (e) The fund consists of:

- 557 (1) money appropriated, credited, or transferred to the fund by the legislature;
- 558 (2) gifts, donations, grants, including federal grants, and any other third-party funds;
- 559 (3) money received by the board for the repayment of a loan made from the fund; and
- 560 (4) interest and other earnings earned on deposits and investments of money in the fund.

561 (f) The account consists of:

- 562 (1) money deposited to the account by the comptroller in the manner prescribed by  
563 subsection (h); and
- 564 (2) interest and other earnings earned on deposits and investments of money in the  
565 account.

566 (g) The Massachusetts Development Finance Agency, in consultation with the executive  
567 office of technology services and security, shall establish a loan program to authorize the board

568 to use money from the fund to provide loans to state agencies for qualifying information  
569 technology modernization projects. A state agency may apply to the board for a loan from the  
570 fund. The application shall include a description of the qualifying information technology  
571 modernization project for which the state agency is requesting a loan. The board may grant a  
572 loan based upon a finding that the project is a qualifying information technology modernization  
573 project. A loan agreement entered into under this subsection shall require the state agency to:

574 (1) repay the loan to the board within seven years of the date the loan is made to the  
575 agency; and

576 (2) make annual reports to the board identifying cost savings realized by the agency as a  
577 result of the project for which the agency received the loan.

578 (h) At the end of each state fiscal year, on the written request of a state agency,  
579 MassDevelopment shall, in conjunction with the comptroller, deposit to the account the  
580 unexpended balance of any money appropriated to the agency for that state fiscal year that is  
581 budgeted by the agency for information technology services or cybersecurity purposes. A state  
582 agency may request money from the account from the board at any time for a qualifying  
583 information technology modernization project.

584 (i) The Massachusetts Development Finance Agency shall separately account for the  
585 amount of money deposited to the account at the request of each state agency under Subsection  
586 (h). Money deposited to the account under subsection (h) and any interest and other earnings on  
587 that money may be provided only to the state agency for which the comptroller deposited the  
588 money to the account and may be used by the agency only for a qualifying information  
589 technology modernization project.

590 (j) Any money deposited to the account at the request of a state agency under subsection  
591 (h) that is not requested by the agency within three years from the date the money is deposited  
592 shall be transferred by the MassDevelopment, in conjunction with the comptroller, to the general  
593 revenue fund to be used in accordance with legislative appropriation.

594 (k) A state agency that receives money from the fund or the account may collaborate with  
595 one or more other state agencies that also receive money from the fund or the account to  
596 purchase information technology systems that may be shared between the agencies.

597 (l) Funds provided to an agency under this section, for any fiscal year, shall be used to  
598 supplement any appropriations made to the agency and shall not supplant any appropriations  
599 made to the agency.

600 (m) MassDevelopment, in consultation with comptroller, MassDevelopment may adopt  
601 rules and regulations to implement and administer this section.

602 SECTION 3. Section 1 of Chapter 639 of the Acts of 1950, as amended by Chapter 54 of  
603 the Acts of 2014, is hereby amended by inserting after the word “causes” the following:-

604 “; or by cybersecurity attack or threat thereof that affects the commonwealth’s critical  
605 infrastructure, information systems owned or operated by the commonwealth, or other  
606 infrastructure or cyber systems deemed necessary and at risk by the governor.”

607 SECTION 4. Section 1 of Chapter 639 of the Acts of 1950, as amended by Chapter 54 of  
608 the Acts of 2014, is hereby further amended by inserting after the definition of “Civil defense”  
609 the following definitions:-

610 “Critical infrastructure”, the assets, systems, and networks, either physical or virtual,  
611 within the commonwealth that are so vital to the commonwealth or the United States that the  
612 incapacitation or destruction of such a system or asset would have a debilitating impact on  
613 cybersecurity, physical security, economic security, the environment, public health or safety or  
614 any combination thereof; provided, however, that “critical infrastructure” shall include, but not  
615 be limited to, election systems, transportation infrastructure, water, gas and electric utilities, and  
616 shall include any critical infrastructure sectors as identified by: (1) Presidential Policy Directive-  
617 21 or successor directive; (2) the federal Cybersecurity and Infrastructure Security Agency; or  
618 (3) the cybersecurity control board.

619 “Cybersecurity attack” shall mean an attack, via electronic means, targeting the  
620 commonwealth’s use of cyberspace for the purpose of infiltrating, disrupting, disabling,  
621 destroying, or maliciously controlling a computing environment or infrastructure; destroying the  
622 integrity of the data; or stealing controlled information.

623 “Cyber System” shall mean the network of hardware, software, procedures, and people  
624 put in place by companies, individuals, or governments that can connect to a network, including  
625 the Internet.

626 SECTION 5. Section 1 of chapter 93H of the General Laws is hereby amended by  
627 inserting after the definition of “Agency” the following definition:-

628 “Biometric information”, a retina or iris scan, fingerprint, voiceprint, map or scan of hand  
629 or face geometry, vein pattern, gait pattern, or other data generated from the specific technical  
630 processing of an individual’s unique biological or physiological patterns or characteristics used



631 to authenticate or identify a specific individual; provided, however, that “biometric information”  
632 shall not include:

633 (i) a digital or physical photograph;

634 (ii) an audio or video recording; or

635 (iii) data generated from a digital or physical photograph, or an audio or video recording,  
636 unless such data is generated to authenticate or identify a specific individual.

637 SECTION 6. Said section 1 of said chapter 93H is hereby further amended by striking out  
638 the definition of “Breach of security” and inserting in place thereof the following definition:-

639 “Breach of security”, the unauthorized acquisition or use of unencrypted electronic data,  
640 or encrypted electronic data when the encryption key or security credential has been acquired;  
641 provided, however, that such unauthorized acquisition or use compromises the security,  
642 confidentiality, or integrity of personal information maintained by a person or agency; and  
643 provided further, that a good faith but unauthorized acquisition of personal information by an  
644 employee or agent of a person or agency for the lawful purposes of such person or agency is not  
645 a breach of security unless the personal information is used in an unauthorized manner or subject  
646 to further unauthorized disclosure.

647 SECTION 7. Said section 1 of said chapter 93H is hereby further amended by inserting  
648 after the definition of “Encrypted” the following definitions:-

649 “Genetic information”, information, regardless of format, that:

650 (i) results from the analysis of a biological sample of an individual, or from another  
651 source enabling equivalent information to be obtained; and

652 (ii) concerns an individual's genetic material, including, but not limited to,  
653 deoxyribonucleic acids (DNA), ribonucleic acids (RNA), genes, chromosomes, alleles, genomes,  
654 alterations or modifications to DNA or RNA, single nucleotide polymorphisms (SNPs),  
655 uninterpreted data that results from analysis of the biological sample or other source, and any  
656 information extrapolated, derived, or inferred therefrom.

657 "Health insurance information", an individual's health insurance policy number,  
658 subscriber identification number, or any identifier used by a health insurer to identify the  
659 individual.

660 "Medical information", information regarding an individual's medical history, mental or  
661 physical condition, or medical treatment or diagnosis by a healthcare professional.

662 SECTION 8. Said section 1 of said chapter 93H is hereby further amended by striking out  
663 the definition of "Personal information" and inserting in place thereof the following definition:-

664 "Personal information" shall mean either of the following:

665 (i) a resident's first name and last name or first initial and last name in combination with  
666 any 1 or more of the following data elements that relate to such resident:

667 (A) social security number;

668 (B) taxpayer identification number or identity protection personal identification number  
669 issued by the Internal Revenue Service;

670 (C) driver's license number, passport number, military identification number, state-issued  
671 identification card number, or other unique identification number issued by the government that  
672 is commonly used to verify the identity of a specific individual;

673 (D) financial account number, or credit or debit card number, with or without any  
674 required security code, access code, personal identification number or password, that would  
675 permit access to a resident's financial account;

676 (E) biometric information;

677 (F) date of birth;

678 (G) genetic information;

679 (H) health insurance information;

680 (I) medical information; or

681 (J) specific geolocation information; or

682 (ii) a username or electronic mail address, in combination with a password or security  
683 question and answer that would permit access to an online account.

684 SECTION 9. Said section 1 of said chapter 93H is hereby further amended by inserting  
685 after the definition of "Personal information" the following definition:-

686 "Specific geolocation information", information derived from technology including, but  
687 not limited to, global positioning system level latitude and longitude coordinates or other  
688 mechanisms that directly identify the specific location of an individual within a geographic area  
689 that is equal to or less than the area of a circle with a radius of 1,850 feet; provided, however,  
690 that "geolocation information" shall exclude the content of communications or any information  
691 generated by or connected to advanced utility metering infrastructure systems or equipment for  
692 use by a utility.

693 SECTION 10. Section 2 of said chapter 93H is hereby amended by inserting the  
694 following subsection:-

695 (d) The rules and regulations adopted pursuant to this section shall be updated from time  
696 to time to reflect any changes to the definitions of “breach of security” or “personal information”  
697 in section 1.

698 SECTION 11. Section 3 of said chapter 93H is hereby amended by inserting after the  
699 words “unauthorized purpose” in subsection (b) the following words:- and such use or  
700 acquisition presents a reasonably foreseeable risk of financial, physical, reputational or other  
701 cognizable harm to the resident.

702 SECTION 12. Said section 3 of said chapter 93H is hereby further amended by striking  
703 out clause (vii) of subsection (b) and inserting in place thereof the following clause:- (vii) the  
704 type of personal information compromised, including, but not limited to, any of the categories of  
705 personal information set forth in subclauses (A) through (J) of clause (i) or in clause (ii) of the  
706 definition of “personal information” in section 1.

707 SECTION 13. Said section 3 of said chapter 93H is hereby further amended by inserting  
708 after the words “attorney general” in subsection (b), the first two times they appear, the  
709 following words each time so appearing:- , Federal Bureau of Investigation.

710 SECTION 14. Said section 3 of said chapter 93H is hereby further amended by striking  
711 out the last sentence of the first paragraph of subsection (b) and inserting in place thereof the  
712 following sentence:- A person who experienced a breach of security shall file a report with the  
713 attorney general and the director of consumer affairs and business regulation certifying their  
714 credit monitoring services comply with section 3A; provided, however, that such a report shall

715 not be required if the personal information compromised by the breach of security is medical  
716 information or specific geolocation information.

717 SECTION 15. Said section 3 of said chapter 93H is hereby further amended by striking  
718 out the third paragraph of subsection (b) and inserting in place thereof the following paragraphs:-

719 The notice to be provided to the resident shall include, but shall not be limited to: (i) the  
720 date, estimated date, or estimated date range of the breach of security; (ii) the type of personal  
721 information compromised, including, but not limited to, any of the categories of personal  
722 information set forth in subclauses (A) through (J) of clause (i) or in clause (ii) of the definition  
723 of “personal information” in section 1; (iii) a general description of the breach of security; (iv)  
724 information that the resident can use to contact the person or agency reporting the breach of  
725 security; (v) the resident’s right to obtain a police report; (vi) how a resident may request a  
726 security freeze and the necessary information to be provided when requesting the security freeze;  
727 (vii) a statement that there shall be no charge for a security freeze; (viii) mitigation services to be  
728 provided pursuant to this chapter; and (ix) the toll-free number, address, and website for the  
729 federal trade commission. The notice shall not be required to include information pursuant to  
730 clauses (vi) and (vii) if the personal information compromised by the breach of security is  
731 medical information or specific geolocation information.

732 The person or agency that experienced the breach of security shall provide a sample copy  
733 of the notice it sent to consumers to the attorney general and the office of consumer affairs and  
734 business regulation. A notice provided pursuant to this section shall not be delayed on grounds  
735 that the total number of residents affected is not yet ascertained. In such case, and where  
736 otherwise necessary to update or correct the information required, a person or agency shall

737 provide additional notice as soon as practicable and without unreasonable delay upon learning  
738 such additional information.

739           If the breach of security involves log-in credentials, pursuant to clause (ii) of the  
740 definition of “personal information” in section 1, for an online account and no other personal  
741 information, the person or agency may comply with this chapter by providing notice in electronic  
742 or other form; provided, however, that such notice shall direct the resident whose personal  
743 information has been breached to: (i) promptly change the resident’s password and security  
744 question or answer, as applicable; or (ii) take other steps appropriate to protect the affected  
745 online account with the person or agency and all other online accounts for which the resident  
746 whose personal information has been breached uses the same username or electronic mail  
747 address and password or security question or answer.

748           If the breach of security involves the log-in credentials, pursuant to clause (ii) of the  
749 definition of “personal information” in section 1, of an electronic mail account furnished by a  
750 person or agency, the person or agency shall not comply with this chapter by providing notice of  
751 the breach of security to such electronic mail address but shall instead provide notice by another  
752 acceptable method of notice pursuant to this chapter or by clear and conspicuous notice delivered  
753 to the resident online when the resident is connected to the online account from an internet  
754 protocol address or online location from which the person or agency knows the resident  
755 customarily accesses the account.

756           SECTION 16. Chapter 140 of the General Laws, as appearing in the 2022 Official  
757 Edition, is hereby amended by inserting after section 131Y the following section:-

758           Section 131Z.

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

761 “Robotic device,” a device capable of locomotion, navigation, movement or flight that  
762 operates at a distance from its operator or supervisor based on commands or in response to  
763 sensor data, or a combination of both, including but not limited to an uncrewed aerial vehicle.

764 “Weapon”, any device designed to threaten or cause death, incapacitation or physical  
765 injury to a person, including but not limited to firearms, chemical agents or irritants,  
766 flamethrowers, kinetic impact projectiles, weaponized lasers and explosive devices.

767 (b) It shall be unlawful for any person, whether or not acting under color of law, to  
768 manufacture, modify, sell, transfer, possess or operate a robotic device equipped or mounted  
769 with a weapon. Whoever knowingly violates the provisions of this subsection shall be punished  
770 by imprisonment in the state prison for not less than 2½ years nor more than 5 years, or in a  
771 house of correction for not less than 18 months nor more than 2 ½ years. Whoever, after having  
772 been convicted of any of the offenses set forth in this subsection, commits a second or  
773 subsequent offense set forth in this subsection, shall be punished by imprisonment in the state  
774 prison for not less than 5 years nor more than 7 years; for a third such offense, by imprisonment  
775 in the state prison for not less than 7 years nor more than 10 years; and for a fourth such offense,  
776 by imprisonment in the state prison for not less than 10 years nor more than 15 years.

777 (c) It shall be unlawful for any person, whether or not acting under color of law, to use a  
778 robotic device to: (A) threaten to commit a crime in violation of section 2 of chapter 275; (B)  
779 criminally harass another person in violation of section 43A of chapter 265; or (C) physically  
780 restrain or to attempt to physically restrain another person. Whoever knowingly violates the

781 provisions of this subsection shall be punished by imprisonment in a house of correction for not  
782 more than 2½ years, by a fine of not more than \$1,000 or by both such fine and imprisonment.  
783 Whoever, after having been convicted of any of the offenses set forth in this subsection, commits  
784 a second or subsequent offense set forth in this subsection, shall be punished by imprisonment in  
785 a house of correction for not more than 2½ years or in a state prison for not more than 10 years,  
786 by a fine of not more than \$15,000 or by both such fine and imprisonment.

787 (d) This section shall not apply to:

788 (i) the United States Department of Defense, or any of its departments, agencies or units,  
789 and the Massachusetts National Guard;

790 (ii) a defense industrial company with respect to robotic devices that are within the scope  
791 of its contract with the department of defense;

792 (iii) a defense industrial company with respect to robotic devices that are within the scope  
793 of its waiver obtained from the attorney general;

794 (iv) robotic devices within the scope of a waiver obtained from the attorney general  
795 solely for the development or testing of technology intended to detect, prevent or mitigate the  
796 unauthorized weaponization of robotic devices; or

797 (v) robotic devices within the scope of a waiver obtained from the attorney general solely  
798 for educational or entertainment purposes.

799 (e) It shall not be a violation of this section for law enforcement agencies or officers, as  
800 those terms are defined in section 1 of chapter 6E, acting in the public performance of their  
801 duties to operate a robotic device equipped or mounted with a weapon or disrupter technology:



802 (i) to destroy, defuse or dispose of explosives or suspected explosives; (ii) for the destruction of  
803 property when there is an imminent threat of death or serious bodily injury; or (iii) for  
804 development, evaluation, testing, education or training relating to the uses permitted in (ii) and  
805 (iii) of this subsection.

806 (f) A law enforcement agency shall be required to obtain a warrant, or other legally  
807 required judicial authorization, prior to deploying a robotic device: (i) onto private property in  
808 any situation in which a warrant would be required if the entry onto that property were made by  
809 an officer; and (ii) to conduct surveillance or location tracking in any situation in which a  
810 warrant or other legally required judicial authorization would be required if such surveillance or  
811 tracking were conducted by an officer or other technology.

812 (g) Any individual may bring a civil action for damages and equitable relief, including  
813 injunctive relief, resulting from a violation of this section or a regulation promulgated under this  
814 section in any court of competent jurisdiction. A plaintiff who prevails in an action under this  
815 section shall be entitled to an award of reasonable attorneys' fees and costs incurred in  
816 connection with said action.

817 (h) Each law enforcement agency shall document, as a public record, each time it uses a  
818 robotic device quarterly to the executive office of public safety and security. Reported  
819 information shall include: the date and time of the use; the scope, target and objective of the use;  
820 whether the robotic device was equipped or mounted with a weapon; the permitted reason for  
821 use; and whether a warrant or other legally required judicial authorization was obtained. The  
822 executive office of public safety and security shall annually, not later than March 31, publicly  
823 report this information on its website.

824 (i) The secretary of the executive office of public safety may promulgate rules and  
825 regulations to carry out the provisions of this section, including rules and regulations related to  
826 the permitted uses of robotic devices equipped or mounted with a weapon by law enforcement  
827 set forth in subsection (e).

828 (j) The attorney general shall promulgate rules and regulations relating to the waivers  
829 described in subsection (d).

830 SECTION 17. Chapter 175 of the general laws is hereby amended by inserting at the end  
831 thereof the following new section:-

832 Section 231. (a) No contract or agreement, including but not limited to, an insurance  
833 contract for cybersecurity insurance, cyber liability insurance, data-breach liability insurance, or  
834 any similar insurance contract, shall prohibit, limit or delay the ability of a party to report a  
835 cybersecurity incident, as defined by section 13 of chapter 7D, or breach of security, as defined  
836 by section 1 of chapter 93H, to any federal, state or local governmental entity.

837 (b) No insurer shall discriminate against an insured party for reporting a cybersecurity  
838 incident, as defined by section 13 of chapter 7D, or breach of security, as defined by section 1 of  
839 chapter 93H, to any federal, state or local governmental entity.

840 SECTION 18. Chapter 29 of the general laws is hereby amended by inserting after  
841 section 2AAAAAA the following new section:-

842 Section 2BBBBBB (a) There is hereby established and set up on the books of the  
843 commonwealth a separate fund to be known as the Cybersecurity Regional Alliances and

844 Multistakeholder Partnerships Pilot Program Fund, hereinafter referred to as the Cybersecurity  
845 Alliances and Partnerships Program Fund.

846 (b) The board of higher education shall hold the Cybersecurity Alliances and Partnerships  
847 Program Fund in an account separate from other funds or accounts. The fund shall be credited  
848 with: (i) revenue from appropriations or other money authorized by the general court and  
849 specifically designated to be credited to the fund; (ii) funds from public and private sources such  
850 as gifts, grants and donations; and (iii) interest earned on such revenues. Any money remaining  
851 in the fund at the end of a fiscal year shall not revert to the General Fund.

852 (c) Amounts credited to the Cybersecurity Alliances and Partnerships Program Fund shall  
853 be used, without further appropriation, by the commissioner of higher education or the  
854 commissioner's designee, under this section for the operation of a Cybersecurity Regional  
855 Alliances and Multistakeholder Partnerships Pilot Program in consultation with participating  
856 industry, non-profits and public higher education institutions. For the purposes of this section  
857 “public higher education institutions” shall include the entities described in section 5 of chapter  
858 15A.

859 (d) An amount not to exceed \$100,000 shall be spent each year to promote the existence  
860 of the Cybersecurity Alliances and Partnerships Program with the goal of attracting and  
861 maximizing industry participation.

862 (e) The public purpose of the Cybersecurity Alliances and Partnerships Program Fund is  
863 to address the cybersecurity workforce gap by:

864 (1) Stimulating cybersecurity education and workforce development by bringing together  
865 stakeholders in the cybersecurity ecosystem;

866 (2) Aligning the cybersecurity workforce needs of employers with the education and  
867 training provided by institutions of higher education;

868 (3) Increasing the pipeline of students pursuing cybersecurity careers; and

869 (4) Developing the cybersecurity workforce to meet industry needs within local or  
870 regional economies.

871 (f) On or before March 1, 2025, the commissioner of higher education shall develop an  
872 application process, selection process, and criteria for public higher education institutions  
873 seeking to participate in the pilot program. Preference shall be given to public higher education  
874 institutions that have or are developing regional pipeline programs in cybersecurity with other  
875 public higher education institutions.

876 (g) The commissioner of higher education shall select any number of public higher  
877 education institutions to participate in the pilot program.

878 (h) Each selected public higher education institution shall:

879 (1) Create a pilot program with goals and metrics;

880 (2) Develop strategies and tactics for building successful regional alliances and  
881 multistakeholder partnerships; and

882 (3) Measure the impact and results of its pilot program and annually share the impact and  
883 results with the commissioner of higher education.

884 (i) The commissioner of higher education shall, not later than July 1, annually report to  
885 the house and senate committees on ways and means, the joint committee on advanced

886 information technologies, the internet and cybersecurity, the joint committee on labor and  
887 workforce development, the joint committee on education and the joint committee on higher  
888 education. The report shall include:

889 (1) The impact and results from each selected public higher education institution pilot  
890 program;

891 (2) Recommendations on how to improve the pilot program;

892 (3) Data on enrollment in the pilot program;

893 (4) Data on how many different groups of people have been served by the pilot program;

894 (5) Data on the number of veterans that have participated in the pilot program;

895 (6) Recommendations on how to recruit more veterans to participate in the pilot program;

896 (7) An annual statement of cash inflows and outflows detailing the sources and uses of  
897 funds;

898 (8) A forecast of future payments based on current binding obligations; and

899 (9) A detailed account of the purposes and amount of administrative costs charged to the  
900 fund.

901 The commissioner of higher education shall include in the annual report a detailed 5 year  
902 review of the Cybersecurity Alliances and Partnerships Program Fund for consideration for  
903 recapitalization.

904 SECTION 19. Notwithstanding any other section of this act, the secretary of technology  
905 services and security shall, to the extent feasible, divide the appointive members of the  
906 cybersecurity control board into three equal groups. Of the appointive members of the  
907 cybersecurity control board, one third shall be designated in their initial appointment to serve for  
908 terms of three years, one third shall be designated for terms of four years, and one third for terms  
909 of five years. Upon the expiration of the initial term of an appointive member, the member or  
910 their successor shall be reappointed or appointed in a like manner for a term of five years. The  
911 secretary shall notify the applicable appointing authority of each appointive member of the  
912 member's initial term duration. Such notice shall be provided no later than 10 days following the  
913 effective date of this act.

914 SECTION 20. Initial appointments to the cybersecurity control board created under this  
915 act shall be made no later than 45 days following the effective date of this act.

916 SECTION 21. The cybersecurity control board created under this act shall promulgate  
917 minimum cybersecurity standards no later than one year from the effective date of this act;  
918 provided that the board shall hold not less than 3 listening sessions in geographically diverse  
919 areas prior to the adoption of such standards.

920 SECTION 22. This act shall take effect upon its passage.