SENATE . . . . . No. 2539

The Commonwealth of Massachusetts

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

SENATE, December 28, 2023.

The committee on Advanced Information Technology, the Internet and Cybersecurity, to whom was referred the petitions (accompanied by bill, Senate, No. 26) of Brendan P. Crighton for legislation to modernize state agency information technology systems; (accompanied by bill, Senate, No. 30) of Barry R. Finegold for legislation to protect sensitive information from security breaches; (accompanied by bill, Senate, No. 31) of Barry R. Finegold for legislation to regulate generative artificial intelligence models like ChatGPT; (accompanied by bill, Senate, No. 32) of Barry R. Finegold for legislation relative to cyber incident response; (accompanied by bill, Senate, No. 35) of Paul W. Mark for legislation to protect against cyber ransom; (accompanied by bill, Senate, No. 36) of Michael O. Moore for legislation to establish a Cybersecurity Control and Review Commission; (accompanied by bill, Senate, No. 37) of Patrick M. O'Connor and Michael J. Soter for legislation to protect the residents of the Commonwealth; (accompanied by bill, Senate, No. 198) of Michael O. Moore for legislation to protect personal identifying information; (accompanied by bill, House, No. 66) of Bradley H. Jones, Jr., and others relative to cyberattack responses; (accompanied by bill, House, No. 76) of Tram T. Nguyen relative to protecting sensitive information from security breaches; (accompanied by bill, House, No. 77) of Angelo J. Puppolo, Jr., that the Office of Information Technology consider cloud computing service options under certain circumstances; (accompanied by bill, House, No. 82) of Michael J. Soter and others for legislation to protect residents of the Commonwealth from the threat posed by certain foreign adversaries using current or potential future social media companies; and (accompanied by bill, House, No. 84) of Marcus S. Vaughn relative to electronic security for certain procurements involving electronic or cyber security equipment components, report the accompanying bill (Senate, No. 2539).

For the committee,
Michael O. Moore

FILED ON: 12/21/2023

SENATE . . . . . No. 2539

The Commonwealth of Massachusetts

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

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:

SECTION 1. Chapter 7D of the general laws is hereby amended by inserting at the end there of the following new sections:-

Section 12. Statewide Cybersecurity Training.

The executive office of technology services and security, in consultation with the office of the comptroller, shall prepare and update from time to time the following online training programs, which the executive office shall publish on its official website: (1) a program which shall provide general cybersecurity training; and (2) special programs, which may be tailored to an entity, profession, role, or other factors that are necessary to further cybersecurity within the commonwealth. Every state, county, and municipal employee shall, within 30 days after becoming such an employee, and every year thereafter, complete the general cybersecurity training, and shall complete such special programs as necessary. Upon completion of the online

training programs, the employee shall provide notice of such completion to be retained for 6 years by the appropriate employer.

The executive office shall consult benchmarks and standards established by the Center for Internet Security, National Institute for Standards and Technology and the Workforce Framework for Cybersecurity in developing the cybersecurity trainings.

The executive office shall establish procedures for implementing this section and ensuring compliance.

For the purposes of this section, the terms state, county, and municipal employee shall have the same meaning as section 1 of chapter 268A.

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 Critical 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.

Section 17. Automated Decision Making Control Board.

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

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

“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.

“Automated decision system”, any computer program, method, statistical model, or process that aims to aid or replace human decision-making using algorithms or artificial intelligence. These systems can include, but are not limited to, analyzing complex datasets about human populations and government services or other activities to generate scores, predictions, warnings, classifications, or recommendations.

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

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

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

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

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

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

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

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

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

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

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

(5) the manner and extent to which covered entities make the automated decision systems they use available to external review, and any existing policies, laws, procedures, or guidelines that may limit external access to data or technical information that is necessary for audits, evaluation, or validation of such systems;

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

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

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

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

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

(v) examine matters related to data sources, data sharing agreements, data security provisions, compliance with data protection laws and regulations, and all other issues related to how data is protected, used, and shared by agencies using automated decision systems, in Massachusetts and in other jurisdictions;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

"Account", the state agency technology upgrades account.

"Board", the Massachusetts innovation fund board.

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

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

"Fund", means the Massachusetts Innovation Fund.

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

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

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

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

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

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

(e) The fund consists of:

(1) money appropriated, credited, or transferred to the fund by the legislature;

(2) gifts, donations, grants, including federal grants, and any other third-party funds;

(3) money received by the board for the repayment of a loan made from the fund; and

(4) interest and other earnings earned on deposits and investments of money in the fund.

(f) The account consists of:

(1) money deposited to the account by the comptroller in the manner prescribed by subsection (h); and

(2) interest and other earnings earned on deposits and investments of money in the account.

(g) The Massachusetts Development Finance Agency, in consultation with the executive office of technology services and security, shall establish a loan program to authorize the board to use money from the fund to provide loans to state agencies for qualifying information technology modernization projects. A state agency may apply to the board for a loan from the fund. The application shall include a description of the qualifying information technology modernization project for which the state agency is requesting a loan. The board may grant a loan based upon a finding that the project is a qualifying information technology modernization project. A loan agreement entered into under this subsection shall require the state agency to:

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

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

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

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

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

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

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

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

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

"; or by cybersecurity attack or threat thereof that affects the commonwealth's critical infrastructure, information systems owned or operated by the commonwealth, or other infrastructure or cyber systems deemed necessary and at risk by the governor."

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

"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 cybersecurity, physical security, economic security, the environment, 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) Presidential Policy Directive-21 or successor directive; (2) the federal Cybersecurity and Infrastructure Security Agency; or (3) the cybersecurity control board.

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

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

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

"Biometric information", a retina or iris scan, fingerprint, voiceprint, map or scan of hand or face geometry, vein pattern, gait pattern, or other data generated from the specific technical processing of an individual's unique biological or physiological patterns or characteristics used to authenticate or identify a specific individual; provided, however, that "biometric information" shall not include:

(i) a digital or physical photograph;

(ii) an audio or video recording; or

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

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

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

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

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

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

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

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

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

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

"Personal information" shall mean either of the following:

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

(A) social security number;

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

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

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

(E) biometric information;

(F) date of birth;

(G) genetic information;

(H) health insurance information;

(I) medical information; or

(J) specific geolocation information; or

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

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

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

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

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

SECTION 11. Section 3 of said chapter 93H is hereby amended by inserting after the words “unauthorized purpose” in subsection (b) the following words:- and such use or

acquisition presents a reasonably foreseeable risk of financial, physical, reputational or other cognizable harm to the resident.

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

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

SECTION 14. Said section 3 of said chapter 93H is hereby further amended by striking out the last sentence of the first paragraph of subsection (b) and inserting in place thereof the following sentence:- A person who experienced a breach of security shall file a report with the attorney general and the director of consumer affairs and business regulation certifying their credit monitoring services comply with section 3A; provided, however, that such a report shall not be required if the personal information compromised by the breach of security is medical information or specific geolocation information.

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

The notice to be provided to the resident shall include, but shall not be limited to: (i) the date, estimated date, or estimated date range of the breach of security; (ii) the type of personal information compromised, including, but not limited to, any of the categories of personal

information set forth in subclauses (A) through (J) of clause (i) or in clause (ii) of the definition of "personal information" in section 1; (iii) a general description of the breach of security; (iv) information that the resident can use to contact the person or agency reporting the breach of security; (v) the resident's right to obtain a police report; (vi) how a resident may request a security freeze and the necessary information to be provided when requesting the security freeze; (vii) a statement that there shall be no charge for a security freeze; (viii) mitigation services to be provided pursuant to this chapter; and (ix) the toll-free number, address, and website for the federal trade commission. The notice shall not be required to include information pursuant to clauses (vi) and (vii) if the personal information compromised by the breach of security is medical information or specific geolocation information.

The person or agency that experienced the breach of security shall provide a sample copy of the notice it sent to consumers to the attorney general and the office of consumer affairs and business regulation. A notice provided pursuant to this section shall not be delayed on grounds that the total number of residents affected is not yet ascertained. In such case, and where otherwise necessary to update or correct the information required, a person or agency shall provide additional notice as soon as practicable and without unreasonable delay upon learning such additional information.

If the breach of security involves log-in credentials, pursuant to clause (ii) of the definition of "personal information" in section 1, for an online account and no other personal information, the person or agency may comply with this chapter by providing notice in electronic or other form; provided, however, that such notice shall direct the resident whose personal information has been breached to: (i) promptly change the resident's password and security question or answer, as applicable; or (ii) take other steps appropriate to protect the affected

online account with the person or agency and all other online accounts for which the resident whose personal information has been breached uses the same username or electronic mail address and password or security question or answer.

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

SECTION 16. Chapter 140 of the General Laws is hereby amended by inserting after section 122D the following section:-

Section 122E.

(a) As used in this section, the following words shall have the following meanings:

"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.

"Robotic device," means a mechanical device capable of action, communication, execution of a task, locomotion, navigation, or movement on the ground and that operates at a distance from its operator(s) or supervisor(s), based on commands, artificial intelligence, machine learning, or in response to sensor data, or a combination of those;

"Uncrewed aircraft" means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft; and

"Weapon" means any device designed to threaten or cause death, incapacitation, or physical injury to any person, including but not limited to stun guns, firearms, machine guns, chemical agents or irritants, kinetic impact projectiles, weaponized lasers, and explosive devices.

(b) Within the commonwealth, it shall be unlawful for any person, whether or not acting under color of law, to manufacture, modify, sell, transfer, or operate a robotic device or an uncrewed aircraft equipped or mounted with a weapon.

(c) Within the commonwealth, it shall be unlawful for any person, whether or not acting under color of law, to use a robotic device or uncrewed aircraft to (i) commit the crime of threats established in section 2 of chapter 275 of the general laws, or (ii) criminally harass another person in terms of section 43A of chapter 265 of the general laws.

(d) Within the commonwealth, it shall be unlawful for any person, whether or not acting under color of law, to use a robotic device or uncrewed aircraft to physically restrain or to attempt to physically restrain a human being.

(e) Whoever knowingly violates the provisions of paragraphs (b), (c), and (d) shall be required to pay a fine of not less than five thousand nor more than twenty-five thousand dollars. Such fine shall be imposed in addition to any other penalty imposed pursuant to the general laws.

(f) This section shall not apply to:

(i) defense industrial companies under contract with the Department of Defense with respect to robotic devices and uncrewed aircraft being developed or produced under that contract;

(ii) to a defense industrial company that obtains a waiver from the Attorney General, as to robotic devices and uncrewed aircraft that are covered by such a waiver; or

(iii) to a robotics company that obtains a waiver from the Attorney General for the purpose of testing anti-weaponization technologies, as to the robotic devices and uncrewed aircraft that are covered by such a waiver.

(g) It shall not be a violation of this section for government officials acting in the public performance of their duties to operate a robotic device or uncrewed aircraft equipped or mounted with a weapon, explosive device, or disrupter technology, when used for the purpose of the disposal of explosives or suspected explosives, for development, evaluation, testing, education or training relating to the use of such technologies for the purpose of disposing of explosives or suspected explosives, or for the destruction of property in cases where there is an imminent, deadly threat to human life.

(h) The secretary of the executive office of public safety may establish rules and regulations relating to the permitted use by government officials of robotic devices equipped

with disruptors or similar technologies. These regulations shall be designed to prevent robotic devices equipped with disruptors or similar technologies from harming or injuring human beings.

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

(j) Any information regarding the use of a robotic device by a law enforcement agency shall become subject to the commonwealth's public records law, with such information made available to the public on request, pursuant to the provisions thereof.

(k) The attorney general may bring an action pursuant to section 4 of chapter 93A to remedy a violation of this section.

(l) Private right of action. Any individual alleging that a violation of this section or a regulation promulgated under this section caused them injury or harm may bring a civil action in any court of competent jurisdiction.

(i) The civil action shall be directed to the agency alleged to have committed the violation or, in the case of an individual, to the person alleged to have committed the violation.

(ii) In a civil action in which the plaintiff prevails, the court may award:—

(a) liquidated damages of not less than five hundred dollars nor more than two thousand dollars;

(b) punitive damages; and

(c) any other relief, including but not limited to an injunction, that the court deems to be appropriate.

(iii) In addition to any relief awarded pursuant to the previous paragraph, the court shall award reasonable attorney's fees and costs to any prevailing plaintiff.

(m) The secretary of the executive office of public safety shall establish such rules and regulations as it may deem necessary to carry out the provisions of this section.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(h) Each selected public higher education institution shall:

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

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

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

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

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

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

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

(3) Data on enrollment in the pilot program;

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

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

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

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

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

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

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

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

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

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

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