SENATE . . . . . No. 2630

The Commonwealth of Massachusetts

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

SENATE, October 16, 2025.

The committee on Advanced Information Technology, the Internet and Cybersecurity to whom was referred the petition (accompanied by bill, Senate, No. 37) of Barry R. Finegold for legislation to promote economic development with emerging artificial intelligence models and safety, report the accompanying bill (Senate, No. 2630).

For the committee,
Michael O. Moore

FILED ON: 10/8/2025

SENATE . . . . . No. 2630

The Commonwealth of Massachusetts

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

An Act promoting economic development with emerging artificial intelligence models and 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 29 of the General Laws is hereby amended by adding the following new section:-

Section 2GGGGGG. Artificial Intelligence Innovation Trust Fund

(a) There shall be established and set up on the books of the commonwealth a separate fund to be known as the Massachusetts Artificial Intelligence Innovation Trust Fund. The secretary of economic development shall be the trustee of the fund and shall, in consultation with the executive director of the Massachusetts Technology Park Corporation established pursuant to chapter 40J, expend money from the fund to: (i) provide grants or other financial assistance to companies developing or deploying artificial intelligence models in key industry sectors as enumerated in line 7002-8070 of section 2 of chapter 238 of the Acts of 2024; provided, however, that the secretary may seek the commitment of matching or other additional funds from private sources before making an expenditure from the fund; (ii) establishment or promotion of artificial intelligence entrepreneurship programs, which may include partnerships with research

institutions in the commonwealth or other entrepreneur support organizations; or (iii) provide grants or other financial assistance for research in artificial intelligence through or in partnership with the Massachusetts Technology Park Corporation.

(b) There shall be credited to the fund an amount equal to: (i) any appropriations or other money authorized by the general court and specifically designated to be credited to the fund; (ii) interest earned on any money in the fund; and (iii) any other grants, premiums, gifts, reimbursements or other contributions received by the commonwealth from any source for or in support of the purposes described in subsection (a).

(c) Amounts credited to the fund may be expended without further appropriation. For the purpose of accommodating timing discrepancies between the receipt of revenues and related expenditures, the fund may incur expenses, and the comptroller shall certify for payment, amounts not to exceed the most recent revenue estimate as certified by the secretary of elder affairs, as reported in the state accounting system. Any money remaining in the fund at the end of a fiscal year shall not revert to the General Fund and shall be available for expenditure in a subsequent fiscal year.

SECTION 2. The General Laws are hereby amended by inserting after chapter 93L the following new chapter:-

CHAPTER 93M. Transparency in Frontier Artificial Intelligence Act

Section 1.

For purposes of this chapter:

(a) “Affiliate” means a person controlling, controlled by, or under common control with a specified person, directly or indirectly, through one or more intermediaries.

(b) “Artificial intelligence model” means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

(c) (1) “Catastrophic risk” means a foreseeable and material risk that a frontier developer’s development, storage, use, or deployment of a frontier model will materially contribute to the death of, or serious injury to, more than 50 people or more than one billion dollars ($1,000,000,000) in damage to, or loss of, property arising from a single incident involving a frontier model doing any of the following:

(A) Providing expert-level assistance in the creation or release of a chemical, biological, radiological, or nuclear weapon.

(B) Engaging in conduct with no meaningful human oversight, intervention, or supervision that is either a cyberattack or, if the conduct had been committed by a human, would constitute the crime of murder, assault, extortion, or theft, including theft by false pretense.

(C) Evading the control of its frontier developer or user.

(2) “Catastrophic risk” does not include a foreseeable and material risk from any of the following:

(A) Information that a frontier model outputs if the information is otherwise publicly accessible in a substantially similar form from a source other than a foundation model.

(B) Lawful activity of the federal government.

(C) Harm caused by a frontier model in combination with other software if the frontier model did not materially contribute to the harm.

(d) "Critical safety incident" means any of the following:

(1) Unauthorized access to, modification of, or exfiltration of, the model weights of a frontier model that results in death or bodily injury.

(2) Harm resulting from the materialization of a catastrophic risk.

(3) Loss of control of a frontier model causing death or bodily injury.

(4) A frontier model that uses deceptive techniques against the frontier developer to subvert the controls or monitoring of its frontier developer outside of the context of an evaluation designed to elicit this behavior and in a manner that demonstrates materially increased catastrophic risk.

(e) (1) "Deploy" means to make a frontier model available to a third party for use, modification, copying, or combination with other software.

(2) "Deploy" does not include making a frontier model available to a third party for the primary purpose of developing or evaluating the frontier model.

(f) "Foundation model" means an artificial intelligence model that is all of the following:

(1) Trained on a broad data set.

(2) Designed for generality of output.

(3) Adaptable to a wide range of distinctive tasks.

(g) “Frontier AI framework” means documented technical and organizational protocols to manage, assess, and mitigate catastrophic risks.

(h) “Frontier developer” means a person who has trained, or initiated the training of, a frontier model, with respect to which the person has used, or intends to use, at least as much computing power to train the frontier model as would meet the technical specifications found in subdivision (i).

(i) (1) “Frontier model” means a foundation model that was trained using a quantity of computing power greater than 10^26 integer or floating-point operations.

(2) The quantity of computing power described in paragraph (1) shall include computing for the original training run and for any subsequent fine-tuning, reinforcement learning, or other material modifications the developer applies to a preceding foundation model.

(j) “Large frontier developer” means a frontier developer that together with its affiliates collectively had annual gross revenues in excess of five hundred million dollars ($500,000,000) in the preceding calendar year.

(k) “Model weight” means a numerical parameter in a frontier model that is adjusted through training and that helps determine how inputs are transformed into outputs.

(l) “Property” means tangible or intangible property.

Section 2.

(a) A large frontier developer shall write, implement, comply with, and clearly and conspicuously publish on its internet website a frontier AI framework that applies to the large

frontier developer's frontier models and describes how the large frontier developer approaches all of the following:

(1) Incorporating national standards, international standards, and industry-consensus best practices into its frontier AI framework.

(2) Defining and assessing thresholds used by the large frontier developer to identify and assess whether a frontier model has capabilities that could pose a catastrophic risk, which may include multiple-tiered thresholds.

(3) Applying mitigations to address the potential for catastrophic risks based on the results of assessments undertaken pursuant to paragraph (2).

(4) Reviewing assessments and adequacy of mitigations as part of the decision to deploy a frontier model or use it extensively internally.

(5) Using third parties to assess the potential for catastrophic risks and the effectiveness of mitigations of catastrophic risks.

(6) Revisiting and updating the frontier AI framework, including any criteria that trigger updates and how the large frontier developer determines when its frontier models are substantially modified enough to require disclosures pursuant to subdivision (c).

(7) Cybersecurity practices to secure unreleased model weights from unauthorized modification or transfer by internal or external parties.

(8) Identifying and responding to critical safety incidents.

(9) Instituting internal governance practices to ensure implementation of these processes.

(10) Assessing and managing catastrophic risk resulting from the internal use of its frontier models, including risks resulting from a frontier model circumventing oversight mechanisms.

(b) (1) A large frontier developer shall review and, as appropriate, update its frontier AI framework at least once per year.

(2) If a large frontier developer makes a material modification to its frontier AI framework, the large frontier developer shall clearly and conspicuously publish the modified frontier AI framework and a justification for that modification within 30 days.

(c) (1) Before, or concurrently with, deploying a new frontier model or a substantially modified version of an existing frontier model, a frontier developer shall clearly and conspicuously publish on its internet website a transparency report containing all of the following:

(A) The internet website of the frontier developer.

(B) A mechanism that enables a natural person to communicate with the frontier developer.

(C) The release date of the frontier model.

(D) The languages supported by the frontier model.

(E) The modalities of output supported by the frontier model.

(F) The intended uses of the frontier model.

(G) Any generally applicable restrictions or conditions on uses of the frontier model.

(2) Before, or concurrently with, deploying a new frontier model or a substantially modified version of an existing frontier model, a large frontier developer shall include in the transparency report required by paragraph (1) summaries of all of the following:

(A) Assessments of catastrophic risks from the frontier model conducted pursuant to the large frontier developer's frontier AI framework.

(B) The results of those assessments.

(C) The extent to which third-party evaluators were involved.

(D) Other steps taken to fulfill the requirements of the frontier AI framework with respect to the frontier model.

(3) A frontier developer that publishes the information described in paragraph (1) or (2) as part of a larger document, including a system card or model card, shall be deemed in compliance with the applicable paragraph.

(4) A frontier developer is encouraged, but not required, to make disclosures described in this subdivision that are consistent with, or superior to, industry best practices.

(d) A large frontier developer shall transmit to the attorney general a summary of any assessment of catastrophic risk resulting from internal use of its frontier models every three months or pursuant to another reasonable schedule specified by the large frontier developer and communicated in writing to the attorney general with written updates, as appropriate.

(e) (1) (A) A frontier developer shall not make a materially false or misleading statement about catastrophic risk from its frontier models or its management of catastrophic risk.

(B) A large frontier developer shall not make a materially false or misleading statement about its implementation of, or compliance with, its frontier AI framework.

(2) This subdivision does not apply to a statement that was made in good faith and was reasonable under the circumstances.

(f) (1) When a frontier developer publishes documents to comply with this section, the frontier developer may make redactions to those documents that are necessary to protect the frontier developer's trade secrets, the frontier developer's cybersecurity, public safety, or the national security of the United States or to comply with any federal or state law.

(2) If a frontier developer redacts information in a document pursuant to this subdivision, the frontier developer shall describe the character and justification of the redaction in any published version of the document to the extent permitted by the concerns that justify redaction and shall retain the unredacted information for five years.

(a) The attorney general shall establish a mechanism to be used by a frontier developer or a member of the public to report a critical safety incident that includes all of the following:

(1) The date of the critical safety incident.

(2) The reasons the incident qualifies as a critical safety incident.

(3) A short and plain statement describing the critical safety incident.

(4) Whether the incident was associated with internal use of a frontier model.

(b) (1) The attorney general shall establish a mechanism to be used by a large frontier developer to confidentially submit summaries of any assessments of the potential for catastrophic risk resulting from internal use of its frontier models.

(2) The attorney general shall take all necessary precautions to limit access to any reports related to internal use of frontier models to only personnel with a specific need to know the information and to protect the reports from unauthorized access.

(c) (1) Subject to paragraph (2), a frontier developer shall report any critical safety incident pertaining to one or more of its frontier models to the attorney general within 15 days of discovering the critical safety incident.

(2) If a frontier developer discovers that a critical safety incident poses an imminent risk of death or serious physical injury, the frontier developer shall disclose that incident within 24 hours to an authority, including any law enforcement agency or public safety agency with jurisdiction, that is appropriate based on the nature of that incident and as required by law.

(3) A frontier developer that discovers information about a critical safety incident after filing the initial report required by this subdivision may file an amended report.

(4) A frontier developer is encouraged, but not required, to report critical safety incidents pertaining to foundation models that are not frontier models.

(d) The attorney general shall review critical safety incident reports submitted by frontier developers and may review reports submitted by members of the public.

(e) (1) The attorney general may transmit reports of critical safety incidents and reports from covered employees to the Legislature, the Governor, the federal government, or appropriate state agencies.

(2) The Attorney General shall strongly consider any risks related to trade secrets, public safety, cybersecurity of a frontier developer, or national security when transmitting reports.

(f) A report of a critical safety incident submitted to the attorney general pursuant to this section, a report of assessments of catastrophic risk from internal use, and a covered employee report are exempt from chapter 66.

(g) (1) Beginning January 1, 2027, and annually thereafter, the attorney general shall produce a report with anonymized and aggregated information about critical safety incidents that have been reviewed by the attorney general since the preceding report.

(2) The attorney general shall not include information in a report pursuant to this subdivision that would compromise the trade secrets or cybersecurity of a frontier developer, public safety, or the national security of the United States or that would be prohibited by any federal or state law.

(3) The attorney general shall transmit a report pursuant to this subdivision to the Legislature and to the Governor.

(h) The attorney general may adopt regulations designating one or more federal laws, regulations, or guidance documents that meet all of the following conditions for the purposes of subdivision (i):

(1) (A) The law, regulation, or guidance document imposes or states standards or requirements for critical safety incident reporting that are substantially equivalent to, or stricter than, those required by this section.

(B) The law, regulation, or guidance document described in subparagraph (A) does not need to require critical safety incident reporting to the Commonwealth of Massachusetts.

(2) The law, regulation, or guidance document is intended to assess, detect, or mitigate the catastrophic risk.

(i) (1) A frontier developer that intends to comply with this section by complying with the requirements of, or meeting the standards stated by, a federal law, regulation, or guidance document designated pursuant to subdivision (h) shall declare its intent to do so to the attorney general.

(2) After a frontier developer has declared its intent pursuant to paragraph (1), both of the following apply:

(A) The frontier developer shall be deemed in compliance with this section to the extent that the frontier developer meets the standards of, or complies with the requirements imposed or stated by, the designated federal law, regulation, or guidance document until the frontier developer declares the revocation of that intent to the attorney general or the attorney general revokes a relevant regulation pursuant to subdivision (j).

(B) The failure by a frontier developer to meet the standards of, or comply with the requirements stated by, the federal law, regulation, or guidance document designated pursuant to subdivision (h) shall constitute a violation of this chapter.

(j) The attorney general shall revoke a regulation adopted under subdivision (h) if the requirements of subdivision (h) are no longer met.

Section 3.

(a) On or before January 1, 2027, and annually thereafter, the attorney general, in consultation with MassCompute, shall assess recent evidence and developments relevant to the purposes of this chapter and shall make recommendations about whether and how to update any of the following definitions for the purposes of this chapter to ensure that they accurately reflect technological developments, scientific literature, and widely accepted national and international standards:

(1) "Frontier model" so that it applies to foundation models at the frontier of artificial intelligence development.

(2) "Frontier developer" so that it applies to developers of frontier models who are themselves at the frontier of artificial intelligence development.

(3) "Large frontier developer" so that it applies to well-resourced frontier developers.

(b) In making recommendations pursuant to this section, the attorney general shall take into account all of the following:

(1) Similar thresholds used in international standards or federal law, guidance, or regulations for the management of catastrophic risk and shall align with a definition adopted in a federal law or regulation to the extent that it is consistent with the purposes of this chapter.

(2) Input from stakeholders, including academics, industry, the open-source community, and governmental entities.

(3) The extent to which a person will be able to determine, before beginning to train or deploy a foundation model, whether that person will be subject to the definition as a frontier developer or as a large frontier developer with an aim toward allowing earlier determinations if possible.

(4) The complexity of determining whether a person or foundation model is covered, with an aim toward allowing simpler determinations if possible.

(5) The external verifiability of determining whether a person or foundation model is covered, with an aim toward definitions that are verifiable by parties other than the frontier developer.

(c) Upon developing recommendations pursuant to this section, the attorney general shall submit a report to the Legislature with those recommendations.

(d) (1) Beginning January 1, 2027, and annually thereafter, the attorney general shall produce a report with anonymized and aggregated information about reports from covered employees that have been reviewed by the attorney general since the preceding report.

(2) The attorney general shall not include information in a report pursuant to this subdivision that would compromise the trade secrets or cybersecurity of a frontier developer, confidentiality of a covered employee, public safety, or the national security of the United States or that would be prohibited by any federal or state law.

(3) The attorney general shall transmit a report pursuant to this subdivision to the Legislature and to the Governor.

Section 4.

(a) A large frontier developer that fails to publish or transmit a compliant document required to be published or transmitted under this chapter, makes a statement in violation of this chapter, fails to report an incident as required by this chapter, or fails to comply with its own frontier AI framework shall be subject to a civil penalty in an amount dependent upon the severity of the violation that does not exceed one million dollars ($1,000,000) per violation.

(b) A civil penalty described in this section shall be recovered in a civil action brought only by the Attorney General.

Section 5.

The loss of value of equity does not count as damage to or loss of property for the purposes of this chapter.

Section 6.

(a) There is hereby established within the Executive Office of Technology Services and Security a consortium that shall develop, pursuant to this section, a framework for the creation of a public cloud computing cluster to be known as “MassCompute.”

(b) The consortium shall develop a framework for the creation of MassCompute that advances the development and deployment of artificial intelligence that is safe, ethical, equitable, and sustainable by doing, at a minimum, both of the following:

(1) Fostering research and innovation that benefits the public.

(2) Enabling equitable innovation by expanding access to computational resources.

(c) The consortium shall make reasonable efforts to ensure that MassCompute is established within public institutions of higher education to the extent possible.

(d) MassCompute shall include, but not be limited to, all of the following:

(1) A fully owned and hosted cloud platform.

(2) Necessary human expertise to operate and maintain the platform.

(3) Necessary human expertise to support, train, and facilitate the use of MassCompute.

(e) The consortium shall operate in accordance with all relevant labor and workforce laws and standards.

(f) (1) On or before January 1, 2027, and annually thereafter, MassCompute shall submit a report from the consortium to the Legislature with the framework, and any updates to said framework, developed pursuant to subdivision (b) for the creation and operation of MassCompute.

(2) The report required by this subdivision shall include all of the following elements:

(A) A landscape analysis of Massachusetts' current public, private, and nonprofit cloud computing platform infrastructure.

(B) An analysis of the cost to the state to build and maintain MassCompute and recommendations for potential funding sources.

(C) Recommendations for the governance structure and ongoing operation of MassCompute.

(D) Recommendations for the parameters for use of MassCompute, including, but not limited to, a process for determining which users and projects will be supported by MassCompute.

(E) An analysis of the state's technology workforce and recommendations for equitable pathways to strengthen the workforce, including the role of MassCompute.

(F) A detailed description of any proposed partnerships, contracts, or licensing agreements with nongovernmental entities, including, but not limited to, technology-based companies, that demonstrates compliance with the requirements of subdivisions (c) and (d).

(G) Recommendations regarding how the creation and ongoing management of MassCompute can prioritize the use of the current public sector workforce.

(g) The consortium shall consist of 14 members as follows:

(1) Four representatives of public and private academic research institutions and national laboratories appointed by the Governor.

(2) Three representatives of impacted workforce labor organizations appointed by the as appointed by Senate President, Speaker of the House of Representatives and Governor, respectively.

(3) Three representatives of stakeholder groups with relevant expertise and experience, including, but not limited to, ethicists, consumer rights advocates, and other public interest advocates appointed by Senate President, Speaker of the House of Representatives and Governor, respectively.

(4) Four experts in technology and artificial intelligence to provide technical assistance appointed by the Governor.

(h) The members of the consortium shall serve without compensation, but shall be reimbursed for all necessary expenses actually incurred in the performance of their duties.

(i) If MassCompute is established within public institutions of higher education, said public institutions of higher education may receive private donations for the purposes of implementing MassCompute.

(k) This section shall be subject to appropriation.

Section 7.

(a) (1) "Catastrophic risk" means a foreseeable and material risk that a frontier developer's development, storage, use, or deployment of a foundation model will materially contribute to the death of, or serious injury to, more than 50 people or more than one billion dollars ($1,000,000,000) in damage to, or loss of, property arising from a single incident involving a foundation model doing any of the following:

(A) Providing expert-level assistance in the creation or release of a chemical, biological, radiological, or nuclear weapon.

(B) Engaging in conduct with no meaningful human oversight, intervention, or supervision that is either a cyberattack or, if committed by a human, would constitute the crime of murder, assault, extortion, or theft, including theft by false pretense.

(C) Evading the control of its frontier developer or user.

(2) “Catastrophic risk” does not include a foreseeable and material risk from any of the following:

(A) Information that a foundation model outputs if the information is otherwise publicly accessible in a substantially similar form from a source other than a foundation model.

(B) Lawful activity of the federal government.

(C) Harm caused by a foundation model in combination with other software where the foundation model did not materially contribute to the harm.

(b) “Covered employee” means an employee responsible for assessing, managing, or addressing risk of critical safety incidents.

(c) “Critical safety incident” means any of the following:

(1) Unauthorized access to, modification of, or exfiltration of the model weights of a foundation model that results in death, bodily injury, or damage to, or loss of, property.

(2) Harm resulting from the materialization of a catastrophic risk.

(3) Loss of control of a foundation model causing death or bodily injury.

(4) A foundation model that uses deceptive techniques against the frontier developer to subvert the controls or monitoring of its frontier developer outside of the context of an evaluation designed to elicit this behavior and in a manner that demonstrates materially increased catastrophic risk.

(a) A frontier developer shall not make, adopt, enforce, or enter into a rule, regulation, policy, or contract that prevents a covered employee from disclosing, or retaliates against a

covered employee for disclosing, information to the Attorney General, a federal authority, a person with authority over the covered employee, or another covered employee who has authority to investigate, discover, or correct the reported issue, if the covered employee has reasonable cause to believe that the information discloses either of the following:

(1) The frontier developer's activities pose a specific and substantial danger to the public health or safety resulting from a catastrophic risk.

(2) The frontier developer has violated this chapter.

(b) A frontier developer shall not enter into a contract that prevents a covered employee from making a disclosure protected under this chapter.

(c) A covered employee may use the hotline described in this section to make reports described in subdivision (a).

(d) A frontier developer shall provide a clear notice to all covered employees of their rights and responsibilities under this section, including by doing either of the following:

(1) At all times posting and displaying within any workplace maintained by the frontier developer a notice to all covered employees of their rights under this section, ensuring that any new covered employee receives equivalent notice, and ensuring that any covered employee who works remotely periodically receives an equivalent notice.

(2) At least once each year, providing written notice to each covered employee of the covered employee's rights under this section and ensuring that the notice is received and acknowledged by all of those covered employees.

(e) (1) A large frontier developer shall provide a reasonable internal process through which a covered employee may anonymously disclose information to the large frontier developer if the covered employee believes in good faith that the information indicates that the large frontier developer's activities present a specific and substantial danger to the public health or safety resulting from a catastrophic risk or that the large frontier developer violated this chapter, including a monthly update to the person who made the disclosure regarding the status of the large frontier developer's investigation of the disclosure and the actions taken by the large frontier developer in response to the disclosure.

(2) (A) Except as provided in subparagraph (B), the disclosures and responses of the process required by this subdivision shall be shared with officers and directors of the large frontier developer at least once each quarter.

(B) If a covered employee has alleged wrongdoing by an officer or director of the large frontier developer in a disclosure or response, subparagraph (A) shall not apply with respect to that officer or director.

(f) The court is authorized to award reasonable attorney's fees to a plaintiff who brings a successful action for a violation of this section.

(g) In a civil action brought pursuant to this section, once it has been demonstrated by a preponderance of the evidence that an activity proscribed by this section was a contributing factor in the alleged prohibited action against the covered employee, the frontier developer shall have the burden of proof to demonstrate by clear and convincing evidence that the alleged action would have occurred for legitimate, independent reasons even if the covered employee had not engaged in activities protected by this section.

(h) (1) In a civil action or administrative proceeding brought pursuant to this section, a covered employee may petition the superior court in any county wherein the violation in question is alleged to have occurred, or wherein the person resides or transacts business, for appropriate temporary or preliminary injunctive relief.

(2) Upon the filing of the petition for injunctive relief, the petitioner shall cause notice thereof to be served upon the person, and thereupon the court shall have jurisdiction to grant temporary injunctive relief as the court deems just and proper.

(3) In addition to any harm resulting directly from a violation of this section, the court shall consider the chilling effect on other covered employees asserting their rights under this section in determining whether temporary injunctive relief is just and proper.

(4) Appropriate injunctive relief shall be issued on a showing that reasonable cause exists to believe a violation has occurred.

(5) An order authorizing temporary injunctive relief shall remain in effect until an administrative or judicial determination or citation has been issued, or until the completion of a review pursuant to this section, whichever is longer, or at a certain time set by the court. Thereafter, a preliminary or permanent injunction may be issued if it is shown to be just and proper. Any temporary injunctive relief shall not prohibit a frontier developer from disciplining or terminating a covered employee for conduct that is unrelated to the claim of the retaliation.

(i) Notwithstanding Massachusetts Rules of Civil Procedure, injunctive relief granted pursuant to this section shall not be stayed pending appeal.

(j) (1) This section does not impair or limit the applicability of provisions of law.

(2) The remedies provided by this section are cumulative to each other and the remedies or penalties available under all other laws of this state.

Section 8.

The loss of value of equity does not count as damage to or loss of property for the purposes of this chapter.

Section 9, The attorney general, in consultation with MassCompute, may promulgate, amend, or rescind regulations for the implementation, administration, and enforcement of this chapter.