STATE OF NEW YORK

10701

IN SENATE

September 18, 2026

Introduced by Sen. FAHY -- read twice and ordered printed, and when printed to be committed to the Committee on Rules

AN ACT to amend the general business law, in relation to independent safety evaluations, monitoring, reporting, security, mitigation, employee protections and enforcement relating to frontier artificial intelligence models

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. This act shall be known and may be cited as the "technical evaluation, risk monitoring, incident notification, AI testing, oversight, and response act" or the "TERMINATOR Act".

§ 2. Section 1420 of the general business law is amended by adding seven new subdivisions 17, 18, 19, 20, 21, 22 and 23 to read as follows:

17. "Independent safety evaluator" means a person or entity that:

(a) possesses technical expertise and experience appropriate to the evaluation of frontier artificial intelligence models and catastrophic risk;

(b) is not an affiliate of the large frontier developer whose frontier model is being evaluated;

(c) has no material financial interest in such large frontier developer other than compensation for services provided in connection with an evaluation required by this article; and

(d) is accredited or otherwise recognized by the office pursuant to standards established by the office.

18. "Material modification" means a modification to a frontier model or the manner in which such model is deployed that could reasonably be expected to materially increase a capability relevant to catastrophic risk or materially reduce the effectiveness of a safeguard designed to prevent or mitigate catastrophic risk.

19. "Significant safety incident" means an event involving a frontier model that materially increases catastrophic risk or provides credible evidence of a capability, vulnerability, failure, circumvention, or compromise of a safety, security, or control mechanism that could materially increase catastrophic risk. A significant safety incident need

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD16379-01-6

not result in death, bodily injury, property damage, or the materialization of catastrophic risk.

20. "Privileged frontier model access" means access to a frontier model that materially exceeds access generally provided to users of such model and that could materially increase catastrophic risk, including access to model weights, internal model checkpoints, a version of a model with safeguards disabled or materially reduced, privileged fine-tuning capabilities, or elevated authority to access external tools, systems, credentials, or computing resources.

21. "Risk-based catastrophic risk monitoring" means a program reasonably designed, in light of the capabilities, deployment context, and reasonably foreseeable uses of a frontier model, to detect significant safety incidents, material changes in capabilities relevant to catastrophic risk, and material failures or circumvention of safeguards designed to prevent or mitigate catastrophic risk.

22. "Tamper-evident" means maintained using technical controls reasonably designed to permit detection of unauthorized alteration or deletion.

23. "Catastrophic harm" means death, serious injury, property damage, or loss of property of the nature and magnitude described in subdivision three of this section arising from conduct described in such subdivision.

§ 3. Paragraph (b) of subdivision 3 of section 1421 of the general business law, as added by chapter 96 of the laws of 2026, is amended to read as follows:

(b) 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 (a) of this subdivision, summaries of all of the following:

(i) assessments of catastrophic risks from the frontier model conducted pursuant to the large frontier developer's frontier AI framework;

(ii) the results of the assessments under subparagraph (i) of this paragraph;

(iii) the extent to which third-party evaluators were involved; [~~and~~]

(iv) other steps taken to fulfill the requirements of the frontier AI framework with respect to the frontier model; and

(v) a summary of the material findings, limitations, uncertainties, identified capabilities, safeguard performance, and identified catastrophic risks contained in any independent safety evaluation required pursuant to section fourteen hundred thirty or fourteen hundred thirty-one of this article. Nothing in this subparagraph shall require publication of information that may be redacted pursuant to subdivision five of this section.

§ 4. Subdivision 2 of section 1422 of the general business law is amended by adding a new paragraph (c), and three new subdivisions 3-a, 3-b and 11 are added to read as follows:

(c) A large frontier developer shall, together with each summary of an assessment of catastrophic risk transmitted pursuant to this subdivision, provide, to the extent reasonably available, technical information reasonably necessary for the office to evaluate the basis for such assessment, including, as applicable, relevant evaluation results, monitoring outputs, model outputs or trajectories, safety or security testing results, and other technical information supporting such assessment.

3-a. (a) A large frontier developer shall report a significant safety incident pertaining to one or more of its frontier models to the office as soon as practicable but in no event later than seven days after determining that such incident has occurred or learning facts sufficient to establish a reasonable belief that such incident has occurred.

(b) Nothing in this subdivision shall alter a more expeditious reporting requirement applicable to a critical safety incident pursuant to subdivision three of this section.

(c) Information submitted pursuant to this subdivision shall be subject to the same confidentiality, disclosure, and information-sharing protections applicable to critical safety incident reports under this section.

(d) No large frontier developer shall knowingly structure or administer its monitoring, incident-review, investigation, or recordkeeping practices for the purpose of avoiding the detection or reporting of a significant safety incident or critical safety incident required to be reported under this article.

3-b. Any report by a large frontier developer of a significant safety incident required pursuant to subdivision three-a of this section or a critical safety incident required pursuant to subdivision three of this section shall include, to the extent reasonably available:

(a) the date and nature of the incident;

(b) the frontier model or models involved;

(c) the capability, vulnerability, safety mechanism, security mechanism, or control implicated by the incident;

(d) the large frontier developer's assessment of the actual or potential consequences of the incident;

(e) corrective or mitigating action taken or planned by the large frontier developer; and

(f) technical information reasonably necessary for the office to assess the nature, cause, and significance of the incident, including, where applicable, relevant logs, model outputs, agent trajectories, tool calls, monitoring outputs, security alerts, and evaluation results.

11. Notwithstanding subdivisions eight and nine of this section, compliance with a federal law, regulation, or guidance document designated by the office as satisfying a reporting requirement under this section shall not relieve a large frontier developer of the obligation to provide the information required pursuant to subdivision three-b of this section, except to the extent that substantially equivalent information has been transmitted to the office pursuant to such federal reporting regime.

§ 5. The general business law is amended by adding seven new sections 1430, 1431, 1432, 1433, 1434, 1435 and 1436 to read as follows:

§ 1430. Independent frontier model safety evaluations. 1. A large frontier developer shall, before first deploying a frontier model in whole or in part in this state, cause an independent safety evaluator to conduct a technical evaluation of such model's capabilities, safeguards, and potential to materially contribute to catastrophic risk.

2. An evaluation required pursuant to this section shall include technical testing, including adversarial testing where appropriate, and shall separately assess where applicable:

(a) capabilities of the underlying frontier model;

(b) capabilities reasonably accessible under the intended deployment configuration; and

(c) the effectiveness and circumvention resistance of safeguards separating underlying capabilities from those reasonably accessible under the intended deployment configuration.

3. An evaluation shall assess, at a minimum:

(a) capabilities that could materially assist in the development, production, or release of chemical, biological, radiological, or nuclear weapons;

(b) offensive cyber capabilities that could materially contribute to catastrophic risk;

(c) capacity to autonomously replicate, propagate, persist, or acquire computing resources or credentials;

(d) capacity to evade, circumvent, or subvert material controls imposed by a developer or user;

(e) capacity to engage in material deceptive behavior, conceal material capabilities, or manipulate or evade safety evaluations or monitoring;

(f) capacity to materially assist in its own development or improvement, or the development or improvement of another frontier model, in a manner that could materially increase catastrophic risk;

(g) effectiveness and resilience of safeguards designed to prevent or mitigate catastrophic risk, including susceptibility of such safeguards to circumvention; and

(h) other capabilities or safeguards relevant to catastrophic risk as the office may designate by regulation.

The requirements of paragraphs (a) through (g) of this subdivision constitute minimum requirements and may not be waived or eliminated by regulation.

4. A large frontier developer shall provide the independent safety evaluator access reasonably necessary to conduct a meaningful technical evaluation, including, where reasonably necessary, access to relevant model checkpoints, interfaces, documentation, testing environments, fine-tuning capabilities, and versions or configurations of the model in which safeguards are disabled or materially reduced.

5. The independent safety evaluator shall prepare a written report describing the methodology, material findings, limitations, uncertainties, identified capabilities, safeguard performance, and identified catastrophic risks. An unredacted copy shall be transmitted to the office.

6. A large frontier developer shall pay the reasonable costs of an evaluation required pursuant to this section. Compensation of an independent safety evaluator shall not be contingent upon the results or conclusions of an evaluation.

7. Nothing in this section shall require or authorize an independent safety evaluator to certify that a frontier model is safe or free from catastrophic risk.

8. (a) The office shall establish by regulation minimum qualifications, technical competency, independence, conflict-of-interest, professional conduct and ethical standards, cybersecurity, confidentiality, personnel-access, information-storage and destruction, and incident-reporting requirements for independent safety evaluators.

(b) Such regulations shall establish standards reasonably designed to ensure the independence, integrity, and professional judgment of independent safety evaluators, including standards governing financial interests, financial dependence, prior or concurrent professional relationships, compensation arrangements, and other circumstances that could reasonably be expected to impair an evaluator's independent professional judgment.

(c) Such regulations shall provide a means for temporary recognition of otherwise qualified evaluators where necessary to ensure adequate evaluator capacity.

9. The office may reject or revoke the accreditation or recognition of an independent safety evaluator upon a finding that such evaluator lacks the technical competence, independence, security practices, professional integrity, or other qualifications required pursuant to this section, and may require a large frontier developer to retain a different independent safety evaluator.

10. The office may determine that an independent technical safety evaluation conducted pursuant to a federal law, regulation, or other governmental regulatory regime satisfies all or part of the requirements of this section where the office determines that such evaluation is substantially equivalent to or more stringent than the requirements of this article. The office may require supplemental evaluation of any capability, safeguard, or risk required to be assessed under this article but not adequately assessed by such evaluation. An evaluation performed solely pursuant to a developer's internal policy or voluntary safety framework shall not qualify under this subdivision solely because such evaluation was conducted or commissioned by the developer.

11. A frontier model deployed in whole or in part in this state before the effective date of this section shall receive the evaluation required by this section within one hundred eighty days after such effective date.

§ 1431. Material modifications and reevaluation. 1. Following the initial evaluation required by section fourteen hundred thirty of this article, a large frontier developer shall cause an additional independent safety evaluation to be conducted before deploying a material modification to a frontier model in whole or in part in this state.

2. A large frontier developer shall make an initial determination as to whether a proposed modification constitutes a material modification. In making such determination, the developer shall consider the cumulative effect of related modifications made since the most recent independent safety evaluation, regardless of whether any individual modification would independently constitute a material modification. The developer shall document the basis for its determination and retain such documentation for not less than five years.

3. The office may review a determination made pursuant to subdivision two of this section. Where the office determines, based upon reasonable evidence, that a modification constitutes a material modification, the office may require an independent safety evaluation.

4. An additional independent safety evaluation shall also be required where:

(a) the developer discovers a material new capability relevant to catastrophic risk;

(b) credible external evidence demonstrates a material catastrophic-risk capability not adequately assessed in a prior evaluation; or

(c) a significant safety incident or critical safety incident reasonably indicates that a prior evaluation or existing safeguard may no longer adequately characterize or mitigate catastrophic risk.

5. An evaluation required pursuant to subdivision four of this section shall be commenced as soon as practicable following the occurrence or discovery of the applicable circumstance and completed within a reasonable period prescribed by the office, taking into account the nature and severity of the potential catastrophic risk.

§ 1432. Post-deployment monitoring. 1. A large frontier developer that deploys a frontier model in whole or in part in this state shall establish, implement, and maintain risk-based catastrophic-risk monitoring for such model to the extent the developer maintains reasonable technical or operational control over the model or deployment.

2. Such monitoring shall, to the extent technically feasible and reasonably necessary in light of the capabilities and deployment context of the model, be designed to detect conduct or events relevant to identifying a significant safety incident, critical safety incident, or material change in catastrophic risk, including:

(a) attempts to circumvent safeguards designed to prevent or mitigate catastrophic risk;

(b) anomalous autonomous behavior;

(c) unauthorized access to or use of external tools, systems, credentials, or computing resources;

(d) unauthorized replication, propagation, or persistence;

(e) material deceptive behavior directed at safety controls, evaluations, or monitoring;

(f) material model-weight security incidents; and

(g) material changes in capabilities relevant to catastrophic risk.

3. Monitoring conducted pursuant to this section shall, to the extent reasonably feasible consistent with the effective detection and investigation of catastrophic risk, minimize the collection and retention of personally identifiable information and ordinary user prompts, responses, and communications unrelated to catastrophic risk.

4. The office may promulgate regulations establishing minimum performance, documentation, data-minimization, security, and review requirements for monitoring required pursuant to this section, provided that such regulations shall be risk-based and proportionate to the capabilities and deployment context of a frontier model.

5. Nothing in this section shall be construed to require generalized monitoring, logging, or retention of the content of ordinary user prompts, responses, or communications.

6. Nothing in this section shall require a large frontier developer to monitor an independently controlled copy or derivative of a frontier model after model weights have been lawfully transferred or publicly released where the developer no longer retains reasonable technical or operational control over such copy or derivative. Nothing in this subdivision shall limit any obligation applicable to the decision to release or transfer model weights under this article.

§ 1433. Tamper-evident safety records. 1. A large frontier developer shall create and maintain tamper-evident records sufficient to reconstruct material actions relevant to catastrophic-risk safety or security, including:

(a) access to, copying of, or transfer of model weights;

(b) material modification, disabling, or removal of safeguards designed to prevent or mitigate catastrophic risk;

(c) deployment or use of a version or configuration of a frontier model with materially reduced safeguards;

(d) privileged frontier model access;

(e) material changes to a frontier model's authority to access external tools, systems, credentials, or computing resources; and

(f) material safety or security alerts and actions taken in response thereto.

2. Records required pursuant to this section shall be retained for not less than five years and shall be protected using reasonable administrative, technical, and physical safeguards against unauthorized access, use, alteration, disclosure, or destruction.

3. Such records shall be made available to the office or attorney general upon request where reasonably necessary to investigate or verify compliance with this article.

4. The office may establish by regulation minimum security and access-control requirements for records required pursuant to this section.

5. Nothing in this article shall require the logging or retention of the content of ordinary user prompts, responses, or communications solely for purposes of compliance with this section.

§ 1434. Privileged frontier model access and model-weight release. 1. A large frontier developer that provides privileged frontier model access shall establish, implement, and maintain a written security program reasonably designed to prevent such access from materially increasing catastrophic risk.

2. Where privileged frontier model access is provided to a third party, the large frontier developer shall, as a condition of providing such access, require by contract that such third party comply with security requirements reasonably appropriate to the nature and level of access provided.

3. The security program required pursuant to subdivision one of this section shall include, as appropriate:

(a) identity verification and access controls;

(b) application of the principle of least privilege;

(c) multifactor or comparably secure authentication;

(d) logging and periodic review of privileged access;

(e) security requirements for systems used to access or store model weights;

(f) credential and key management;

(g) procedures for prompt suspension or revocation of access; and

(h) incident detection and reporting.

4. A large frontier developer shall maintain reasonable procedures to verify compliance with the requirements of this section and shall promptly suspend or modify privileged frontier model access where it reasonably determines that continued access would create a material and unreasonable risk of catastrophic harm.

5. Prior to publicly releasing, broadly distributing, or otherwise transferring model weights in a manner reasonably expected to materially diminish the developer's ability to maintain or enforce safeguards against catastrophic risk, a large frontier developer shall ensure that the consequences of such release or transfer have been assessed as part of an independent safety evaluation required pursuant to this article. Such evaluation shall consider, as applicable, the extent to which safeguards may become unavailable, removable, or circumventable following the release or transfer and the reasonably foreseeable catastrophic risks arising from the inability of the developer to control downstream copies or derivatives.

6. The office shall promulgate regulations establishing minimum cybersecurity standards pursuant to this section and shall, to the extent practicable, consider applicable federal standards and generally accepted cybersecurity practices.

§ 1435. Mitigation of material and unreasonable catastrophic risk. 1. Where an independent safety evaluation, significant safety incident, critical safety incident, post-deployment monitoring, or other credible evidence provides a reasonable basis to determine that deployment or operation of a frontier model presents a material and unreasonable risk of catastrophic harm, a large frontier developer shall implement safeguards reasonably sufficient to mitigate such risk.

2. In determining whether a risk is material and unreasonable, the office shall consider, as applicable:

(a) the severity and scale of reasonably foreseeable harm;

(b) the likelihood of such harm based upon available technical and empirical evidence;

(c) demonstrated capabilities of the frontier model;

(d) accessibility of a capability relevant to catastrophic risk;

(e) effectiveness, resilience, and circumvention resistance of applicable safeguards;

(f) degree of autonomy of the model and its access to external tools, systems, credentials, or computing resources;

(g) context and scale of deployment; and

(h) reasonably foreseeable misuse.

3. The mere theoretical possibility that a frontier model could contribute to catastrophic harm shall not, standing alone, constitute a material and unreasonable risk of catastrophic harm.

4. Where the office determines, based upon reasonable evidence, that a frontier model presents a material and unreasonable risk of catastrophic harm, the office may require additional independent evaluation, enhanced monitoring or reporting, or additional or modified technical or administrative safeguards reasonably necessary and proportionate to the identified risk.

5. Where the office determines that a specific capability, tool, deployment configuration, privileged-access arrangement, or transfer or distribution of model weights presents a material and unreasonable risk of catastrophic harm, the office may temporarily restrict such activity upon written findings that:

(a) identify the material and unreasonable risk;

(b) identify the evidence supporting such determination;

(c) establish a direct relationship between the activity restricted and the identified risk; and

(d) determine that less restrictive measures would be inadequate to reasonably mitigate such risk.

6. Except as provided in subdivision seven of this section, prior to imposing a restriction pursuant to subdivision five of this section, the office shall provide the large frontier developer with notice of the proposed restriction, the material basis therefor, and a reasonable opportunity to respond.

7. Where the office determines that providing prior notice and an opportunity to respond would materially increase an imminent risk of catastrophic harm, the office may impose a restriction pursuant to subdivision five of this section without prior notice. The office shall promptly thereafter provide the developer with the written findings supporting such restriction and an expedited opportunity to respond and seek review.

8. A restriction imposed pursuant to subdivision five or seven of this section shall remain effective for no longer than thirty days unless renewed by the office upon updated written findings satisfying the requirements of subdivision five of this section. Where a restriction imposed pursuant to subdivision five or seven of this section remains in effect for more than sixty days in the aggregate, the office shall refer the matter to the attorney general for review. Such referral shall not require the attorney general to commence an action, shall not independently alter the duration or validity of the restriction, and shall not

limit the authority of the office to renew such restriction in accordance with this subdivision.

9. In determining an appropriate measure under this section, the office shall consider the availability and likely effectiveness of less restrictive measures. Nothing in this subdivision shall require the office to impose or exhaust a less restrictive measure that it reasonably determines would be inadequate.

10. Where the office determines, based upon substantial evidence, that deployment or operation of a frontier model presents an imminent and unreasonable risk of catastrophic harm and that less restrictive measures would be inadequate, the office may refer such determination to the attorney general.

11. Upon a referral pursuant to subdivision ten of this section, the attorney general may commence an action in the supreme court for temporary or permanent injunctive relief necessary and proportionate to prevent or mitigate such risk, including, where necessary, restriction of deployment or operation of the frontier model in this state.

§ 1436. Protected safety disclosures and independent safety research. 1. No large frontier developer, or contractor or subcontractor thereof, shall discharge, demote, suspend, threaten, harass, discriminate, or otherwise retaliate against an employee or contractor because such employee or contractor, based upon a reasonable belief, discloses information concerning:

(a) a violation of this article;

(b) a significant safety incident or critical safety incident;

(c) a material misrepresentation or omission concerning an independent safety evaluation, frontier AI framework, or compliance with this article;

(d) interference with or manipulation of an independent safety evaluation; or

(e) a material and unreasonable risk of catastrophic harm.

2. The protections of this section shall apply to a disclosure made to the large frontier developer, an independent safety evaluator, the office, the attorney general, or an appropriate federal, state, or local governmental entity.

3. No agreement, policy, form, or condition of employment or contracting may prohibit or restrict a disclosure protected by this section. Any such provision shall be void and unenforceable to the extent of such prohibition or restriction.

4. The office shall establish a secure mechanism through which an employee or contractor may confidentially report alleged retaliation or information described in subdivision one of this section. The office may investigate such complaint, request or obtain information reasonably necessary to assess the complaint pursuant to its authority under this article, and refer its findings to the attorney general.

5. A violation of this section shall constitute a violation of this article enforceable by the attorney general. In an action brought pursuant to this article, the attorney general may seek, in addition to any other relief authorized by law, reinstatement, back pay, lost compensation, restitution, injunctive relief, and other equitable relief reasonably necessary to remedy retaliation.

6. Nothing in this section shall be construed to create a private right of action.

7. Nothing in this article shall be construed to prohibit or impose liability solely because a person conducts authorized, good-faith safety or security research in accordance with applicable law and reasonable

security controls. Nothing in this subdivision shall exempt any person from otherwise applicable requirements relating to unauthorized access, disclosure of protected information, or conduct creating a material and unreasonable risk of catastrophic harm.

§ 6. Section 1427 of the general business law is amended by adding five new subdivisions 4, 5, 6, 7 and 8 to read as follows:

4. In addition to any other penalty authorized by this article, the attorney general may bring a civil action to recover a civil penalty not to exceed one-half of one percent of annual gross revenue where a large frontier developer knowingly:

(a) falsifies or materially conceals information required to be reported or transmitted pursuant to this article;

(b) conceals a significant safety incident required to be reported pursuant to this article;

(c) destroys, alters, or causes the destruction or alteration of a record required to be maintained pursuant to this article for the purpose of impeding oversight or enforcement;

(d) materially interferes with an independent safety evaluation required pursuant to this article;

(e) denies an independent safety evaluator access that such developer knows is required pursuant to this article; or

(f) coerces, threatens, or retaliates against a person for the purpose of preventing a report, disclosure, or transmission required or protected by this article.

5. The attorney general may bring a civil action to recover a civil penalty not to exceed one percent of annual gross revenue where a large frontier developer:

(a) willfully conceals a critical safety incident required to be reported pursuant to this article; or

(b) willfully and repeatedly engages in conduct described in subdivision four of this section with the specific intent to conceal material information or frustrate oversight or enforcement under this article.

6. For purposes of subdivisions four and five of this section, "annual gross revenue" means the gross revenue, during the most recently completed fiscal year preceding the violation, of the large frontier developer and any affiliate that materially participated in, controlled, directed, or provided material support for the development, deployment, operation, distribution, or provision of access to the frontier model giving rise to the violation.

7. Where the attorney general establishes that a reorganization, transfer of assets, allocation of revenue, change in corporate form, creation or use of an affiliate, or other transaction or arrangement was undertaken in substantial part for the purpose of avoiding or materially reducing a penalty authorized by this section, the court may determine annual gross revenue without regard to such transaction or arrangement to the extent necessary to prevent such evasion.

8. A good-faith legal, scientific, or technical disagreement concerning whether an incident is reportable, whether information or access is required or reasonably necessary under this article, or the nature or severity of a risk shall not, standing alone, constitute concealment, obstruction, or interference for purposes of subdivisions four or five of this section.

§ 7. Subdivision 4 of section 1428 of the general business law, as added by chapter 96 of the laws of 2026, is amended to read as follows:

4. Large frontier developers shall be assessed in pro rata shares by the department to defray the operating expenses, including all direct

and indirect costs, of administering the obligations imposed by this article. **Such costs may include, but shall not be limited to, costs associated with the accreditation, recognition, and oversight of independent safety evaluators; technical personnel; contracts with technical experts, laboratories, academic institutions, or other qualified entities; investigations; rulemaking; post-deployment monitoring oversight; information security; and enforcement.**

§ 8. Section 1429 of the general business law, as added by chapter 96 of the laws of 2026, is amended to read as follows:

§ 1429. Rulemaking authority. **1.** The office is hereby authorized to adopt rules and regulations to implement the provisions of this article as needed. To the extent the office determines that doing so will facilitate safety and transparency consistent with the underlying purpose of this article, the office may consider additional reporting or publication requirements for information to facilitate safety and transparency, including but not limited to, post-critical safety incident information, sharing plans and protocols, and the transmission of frontier AI frameworks to the office.

2. The office may promulgate such additional rules and regulations as are necessary to implement sections fourteen hundred thirty through fourteen hundred thirty-six of this article.

3. In promulgating and periodically reviewing rules and regulations pursuant to this article, the office shall consult, as appropriate, with federal agencies and standard-setting bodies, independent technical experts, academic institutions, civil society organizations, frontier developers, independent safety evaluators, cybersecurity experts, and other persons with relevant expertise.

4. The office may enter into contracts or agreements with technical experts, laboratories, academic institutions, or other qualified entities as reasonably necessary to administer and enforce this article. Nothing in this subdivision shall authorize the office to delegate to a private entity a final regulatory or enforcement determination vested in the office by this article.

5. The office may adopt procedures governing determinations of substantial equivalence pursuant to section fourteen hundred thirty of this article and may enter into appropriate information-sharing or cooperative arrangements with federal agencies or other governmental regulators, provided that confidential information remains subject to protections required by this article and applicable law.

§ 9. Severability. If any clause, sentence, paragraph, subdivision, section, or part of this act, or the application thereof to any person or circumstance, shall be adjudged by any court of competent jurisdiction to be invalid, such judgment shall not affect, impair, or invalidate the remainder thereof or the application thereof to other persons or circumstances.

§ 10. This act shall take effect one year after it shall have become a law; provided, however, that if chapter 96 of the laws of 2026 shall not have taken effect on or before such date then this act shall take effect one year after such chapter takes effect.