....
(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. ______

To provide for Federal oversight of the development and deployment of frontier artificial intelligence in interstate and foreign commerce, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. OBERNOLTE introduced the following bill; which was referred to the Committee on ______________________________

A BILL

To provide for Federal oversight of the development and deployment of frontier artificial intelligence in interstate and foreign commerce, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Frontier Risk Oversight, National Transparency, Independent Evaluation, and Reporting Act'' or the ''FRONTIER Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) ACCEPTABLE LEVELS OF CATASTROPHIC RISK MITIGATION.—The term ‘‘acceptable levels of catastrophic risk mitigation’’ means risk mitigation adequate to ensure that the anticipated benefits of a frontier model made available or used in interstate or foreign commerce outweigh its level of catastrophic risk, taking into consideration the probability and magnitude of the model's anticipated benefits and catastrophic risks.

(2) AFFILIATE.—The term ‘‘affiliate’’ means an entity that satisfies any of the following requirements:

(A) Controls another entity through an intermediary.

(B) Is through such intermediary controlled by such other entity.

(C) Is through such intermediary under common control with such other entity.

(3) AI; ARTIFICIAL INTELLIGENCE; ARTIFICIAL INTELLIGENCE MODEL.—The terms ‘‘AI’’, ‘‘artificial intelligence’’, and ‘‘artificial intelligence model’’ have the meaning given such terms in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(4) AI-RELATED DEVELOPMENT EXPENDITURES.—The term “AI-related development expenditures” means amounts paid or incurred in interstate or foreign commerce, without regard to whether such amounts are expensed, capitalized, deducted, or amortized for financial reporting or tax purposes, that are attributable to artificial intelligence development, training, fine-tuning, modification, security, or evaluation.

(5) ASSESSMENT.—The term “assessment” means a review conducted by an IVO licensed under section 5 to assess the adequacy of a very large frontier developer’s frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks for achieving acceptable levels of catastrophic risk mitigation.

(6) CATASTROPHIC RISK.—The term “catastrophic risk” means—

(A) 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 $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:

(i) providing, in the development or release of a chemical, biological, radiological, nuclear, or cyber weapon, assistance that is not publicly available;

(ii) engaging in conduct with no meaningful human oversight or intervention, that—

(I) is a cyberattack; or

(II) if such conduct is committed by an individual, would constitute murder, assault, extortion, or theft, including such theft by false pretense; or

(iii) evading control of such developer or a user of such model; and

(B) does not include a foreseeable and material risk from any of the following:

(i) 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;

(ii) lawful activity of the Federal Government; or

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

(7) CRITICAL SAFETY INCIDENT.—The term "critical safety incident" means any of the following:

(A) Unauthorized access to, modification of, or exfiltration of, the model weights of a frontier model.

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

(C) Loss of control of such model.

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

(8) DEPLOY.—The term "deploy" means—

(A) to make a frontier model available in interstate or foreign commerce to a third party for use, modification, copying, or combination with other software; and

(B) does not include making such model available to such third party for the primary purpose of developing or evaluating such model.

(9) FOUNDATION MODEL.—The term ‘‘foundation model’’ means an artificial intelligence model made available or used in interstate or foreign commerce that is all of the following:

(A) Trained on a broad data set.

(B) Designed for generality of output.

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

(10) FRONTIER AI FRAMEWORK.—The term ‘‘frontier AI framework’’ means documented technical and organizational protocols to manage, assess, and mitigate catastrophic risks.

(11) FRONTIER DEVELOPER.—The term ‘‘frontier developer’’ means an entity operating in interstate or foreign commerce that has trained, or initiated the training of, a frontier model using a quantity of computing power that meets the technical specifications set forth in subsection (l).

(12) FRONTIER MODEL.—The term ‘‘frontier model’’ means a foundation model that was trained using a quantity of computing power greater than 10✖26 integer or floating-point operations. The

quantity of computing power described in this paragraph includes computing for the original training run and for any subsequent fine-tuning, reinforcement learning, or other substantial modification the developer applies to a preceding foundation model.

(13) IMMINENT CATASTROPHIC RISK.—The term ''imminent catastrophic risk'' means a present or impending catastrophic risk.

(14) IVO.—The term ''IVO'' means an independent verification organization operating in interstate or foreign commerce that is licensed under subsection (c) of section 5 and the regulations prescribed under subsection (c) of section 3.

(15) LARGE FRONTIER DEVELOPER.—The term ''large frontier developer'' means a frontier developer that, together with its affiliates, collectively, during the preceding 36-month period, determined as of the first day of each calendar month, both—

(A) had gross revenues in excess of $50,000,000; and

(B) incurred not less than $1,000,000,000 in AI-related development expenditures.

(16) MATERIAL MODIFICATION.—The term ''material modification'' means with respect to a frontier AI framework, a significant change to such

framework, including a significant change in the assessment, mitigation, or management of catastrophic risk carried out pursuant to such framework.

(17) MODEL WEIGHT.—The term "model weight" means a numerical parameter that satisfies the following requirements:

(A) Is in a frontier model.

(B) Is adjusted through training.

(C) Facilitates the determination of how input data for such model is transformed into an output of such model.

(18) PROPERTY.—The term "property" includes—

(A) tangible or intangible property; and

(B) does not include the loss of value of equity.

(19) SECRETARY.—The term "Secretary" means the Secretary of Commerce.

(20) SUBSTANTIAL MODIFICATION.—The term "substantial modification" means with respect to a frontier model, a significant change in how such model is deployed, such as enabling a new fine-tuning capability for, releasing a model weight of, or adding a new feature to such model, that neces-

sitates for such model an assessment of catastrophic risk.

(21) UNDER SECRETARY.—The term ''Under Secretary'' means the Under Secretary of Commerce for AI Security, who shall be appointed by the Secretary.

(22) VERY LARGE FRONTIER DEVELOPER.—The term ''very large frontier developer'' means a frontier developer that, together with its affiliates, collectively, during the preceding 36-month period, determined as of the first day of each calendar month, both—

(A) had gross revenues in excess of $5,000,000,000; and

(B) incurred not less than $10,000,000,000 in AI-related development expenditures.

SEC. 3. RULEMAKING.

(a) PROCEDURE.—Each regulation prescribed under this Act shall be prescribed in accordance with section 553 of title 5, United States Code.

(b) FRAMEWORK REQUIREMENTS.—

(1) DEADLINE.—Not later than 180 days after the date of enactment of this Act, the Under Secretary shall issue, and thereafter update as appro-

priate, regulations establishing minimum requirements for frontier AI frameworks.

(2) CONTENTS.—Regulations issued under this subsection shall, at a minimum, address each of the requirements of section 4(a).

(3) PERIODIC REVIEW.—The Under Secretary shall review the regulations issued under this subsection not less frequently than once every year, and shall update such regulations as the Under Secretary determines to be necessary or appropriate.

(c) IVO LICENSING AND OVERSIGHT.—Not later than 180 days after the date of enactment of this Act, the Under Secretary shall prescribe regulations necessary to carry out the licensing and oversight of IVOs under section 5, which shall include the following:

(1) Conflict-of-interest and funding-transparency requirements, including reporting requirements regarding the IVOs' funding sources and revenue generation and self-audit requirements regarding the IVOs' personnel and leadership to ensure adequate independence from the artificial intelligence industry.

(2) Procedures and requirements for entities to apply for licensure as an IVO, including the following:

(A) Procedures and requirements for the applicant to submit a plan to the Under Secretary detailing—

(i) the benchmarks, technologies, metrics, and methodologies the applicant proposes using to assess the adequacy of the frontier developer's frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks, to ensure acceptable levels of catastrophic risk mitigation;

(ii) the applicant's proposed procedure for prescribing and assessing implementation of corrective action to remedy any identified deficiency in achieving acceptable levels of catastrophic risk mitigation;

(iii) the applicant's proposed methodology for ensuring that the benchmarks, technologies, metrics, and methodologies proposed in clause (i) keep pace with technological and organizational changes in frontier model development;

(iv) any subcontractors that the applicant proposes to use to carry out its responsibilities under this Act; and

(v) the technical qualifications of the personnel the applicant proposes to use to conduct assessments and of any subcontractor the applicant plans to engage under subsection (d) of section 5 to perform any portion of an assessment.

(B) Findings required for the Under Secretary to license an applicant as an IVO, including—

(i) that the applicant has demonstrated its independence from the artificial intelligence industry;

(ii) that every element of the applicant's plan is adequate to ensure that frontier models assessed by the IVO achieve acceptable levels of catastrophic risk mitigation; and

(C) Findings that require the Under Secretary to revoke an IVO's license, including—

(i) that the IVO's plan is materially misleading or inaccurate;

(ii) that the IVO fails to adhere to its plan in a manner that materially impairs its ability to fulfill its responsibilities;

(iii) that a material change compromises the IVO's independence from the artificial intelligence industry;

(iv) that models verified by the IVO fail to achieve or have failed to achieve acceptable levels of catastrophic risk mitigation, unless the IVO demonstrates that—

(I) the IVO identified the relevant failure, deficiency, or material weakness in an assessment report submitted under subsection (f) of section 5 or a supplemental report submitted under subsection (i) of such section, and recommended corrective actions adequate to achieve acceptable levels of catastrophic risk mitigation; and

(II) such failure is attributable to the very large frontier developer's failure to implement such corrective actions, and not to any deficiency in the IVO's assessment, methods, or performance of its obligations under section 5;

(v) that evolution of technology renders the IVO's methods obsolete for verifying acceptable mitigation of catastrophic risk; and

(vi) that the IVO has failed to comply with its obligations under section 5.

(D) Procedures for the formation of expert panels with respect to one or more specific catastrophic risks to advise the Under Secretary on the issuance and revocation of IVO licenses.

(3) Minimum requirements for assessments, taking into account relevant approaches, best practices, frameworks, and methods.

(4) Provisions regarding circumstances mandating corrective action or loss of license.

(5) Rules regarding the submission and processing of assessment reports, including a secure method for submission of assessment reports under subsection (f), subsection (g), and subsection (i) of section 5 and other sensitive information, and a process for securely processing sensitive information and protecting trade secrets.

(6) Any other rules reasonably necessary to the administration of the IVO oversight and licensing regime described in section 5.

(d) Modification Criteria.—Not later than 180 days after the date of enactment of this Act, the Under Secretary shall prescribe regulations establishing criteria for determining whether a modification to a frontier model constitutes a substantial modification within the meaning of subsection (t) of section 2, and whether a modification to a frontier AI framework constitutes a material modification within the meaning of subsection (p) of section 2.

(e) Procedures for Reports, Redactions, and State Opt-in.—The Under Secretary may prescribe regulations establishing—

(1) the approaches, formats, and procedures applicable to publications, reports, and submissions required under sections 4 and 5;

(2) procedures applicable to redactions made under subsection (f) of section 4 and subsection (m) of section 5, including standards for justifications required under subsection (f)(2) of section 4 and subsection (m)(2) of section 5; and

(3) the form, manner, and procedures applicable to the opt-in by State Attorneys General under subsection (i) of section 4 and subsection (k) of section 5, including the secure transmission to opted-in

State Attorneys General of the reports and referrals covered by such opt-ins.

(f) UPDATES TO COVERAGE THRESHOLDS.—

(1) AUTHORITY.—The Under Secretary may by regulation increase—

(A) the threshold quantity of computing power specified in subsection (l) of section 2; or

(B) the threshold amounts of gross revenues and AI-related development expenditures specified in subsections (o) and (v) of section 2.

(2) CRITERIA.—The Under Secretary shall set each threshold at the level the Under Secretary determines is best calculated to ensure that the terms defined in subsections (k), (l), (o), and (v) of section 2 encompass the artificial intelligence models and developers whose activities present catastrophic risk, and do not encompass those whose activities do not, taking into account advances in algorithmic and hardware efficiency, changes in the cost of developing and training foundation models, inflation, and the anticipated effect of the modification on the entities subject to sections 5 and 6.

(3) PERIODIC REVIEW.—Not less frequently than once every 2 years, the Under Secretary shall review the thresholds described in paragraph (1), de-

termine whether an increase is warranted, and publish the determination and its basis on a website of the Department of Commerce.

(4) PROSPECTIVE APPLICATION.—A regulation prescribed under this subsection shall take effect not earlier than 180 days after publication in final form and shall apply only with respect to obligations arising on or after its effective date.

SEC. 4. TRANSPARENCY AND REPORTING.

(a) FRONTIER AI FRAMEWORK.—Not later than one year after the date of enactment of this Act, or 90 days after a developer first qualifies as a large frontier developer, whichever is later, a large frontier developer shall write, implement, comply with, and clearly and conspicuously publish on a publicly available website of such developer a frontier AI framework that satisfies the following requirements:

(1) Applies to each frontier model of such developer.

(2) Includes information relating to how such developer carries out the following:

(A) Incorporating into such framework widely-accepted national, international, and industry approaches, best practices, frameworks, and methods for risk mitigation.

(B) Identifying risk thresholds utilized by such developer to assess whether each such model has a capability that could pose a catastrophic risk.

(C) Assessing whether, based upon such thresholds, each model has a capability that could pose a catastrophic risk.

(D) Reviewing the results of such assessment and such mitigation to determine—

(i) whether to deploy such model; and

(ii) whether to internally utilize such model.

(E) Utilizing a third party to assess the risk that such risk thresholds will be exceeded and the effectiveness of such mitigation.

(F) Reviewing and updating such framework, including the criteria in such framework that prompt such updating and the process through which such developer determines whether such model includes a substantial modification, such that a disclosure is required pursuant to subsection (d).

(G) Cybersecurity to secure nonpublic model weights from unauthorized modification or transfer.

(H) Identifying and responding to a critical safety incident related to such developer.

(I) Implementing internal governance practices to ensure implementation of such framework.

(b) UPDATES.—

(1) IN GENERAL.—Not less frequently than annually after a large frontier developer publishes a frontier AI framework pursuant to subsection (a), such developer shall carry out the following:

(A) Review and, if such developer determines appropriate, update such framework.

(B) If such framework is so updated, publish on a publicly available website of such developer such framework, as so updated.

(2) MATERIAL MODIFICATION.—If a large frontier developer makes a material modification to the frontier AI framework of such developer published pursuant to subsection (a), not later than 30 days after the date of such modification, such developer shall publish on a publicly available website a justification for such modification.

(c) COMPLIANCE AUDIT.—Not later than one year after the date of enactment of this Act, or 90 days after a developer first qualifies as a large frontier developer, whichever is later, and annually thereafter, a large frontier developer shall retain a third party to perform an independent audit of compliance with the frontier AI framework of such developer published pursuant to subsection (a). The third party shall conduct the audit consistent with generally accepted auditing approaches, best practices, frameworks, and methods and shall possess demonstrated competence to perform the audit, including experience employing or contracting with individuals who possess technical expertise in the safety of frontier models. A large frontier developer shall not retain a third party if either the developer or the third party has a financial interest in the other. A large frontier developer may compensate a third party for its services but shall not condition any payment, or the amount of any payment, on the results of the third party's audit.

(1) ACCESS.—The third party shall be granted timely access to all materials, records, personnel, systems, and all other information reasonably necessary to comply with its obligations under this subsection, including all unredacted versions of materials published pursuant to this Act. To protect the developer's trade secrets and confidential business information, cybersecurity, national security of the United States, or public safety, a large frontier de-

veloper may impose security protocols on the third party, including restrictions on note-taking, copying, retaining, or removing materials, requirements for on-premises review, and confidentiality requirements.

(2) REPORT CONTENTS.—The third party shall produce a report that includes all of the following:

(A) A description of whether the large frontier developer has substantially complied with the frontier AI framework of such developer.

(B) If applicable, a description of material deviations from such framework, an explanation of any deviation and its rationale, and any recommendations for how the developer can improve its policies and processes for ensuring compliance with such framework.

(C) A detailed assessment of the large frontier developer's internal controls, including its designation and empowerment of senior personnel responsible for implementation of such framework by the developer, its employees, and its contractors.

(D) A list of the personnel involved in the audit.

(E) The third party's procedures for managing conflicts of interest and any conflicts of interest of personnel involved in the audit.

(F) The methodology of the audit and the nature of the information reviewed to conduct the audit.

(G) The signature of the lead auditor certifying the results of the audit.

(3) RETENTION.—A large frontier developer shall retain an unredacted copy of the report required under paragraph (2) for as long as a frontier model of such developer is deployed, plus 5 years.

(4) PUBLICATION AND TRANSMITTAL.—Not later than 30 days after receiving the audit report, a large frontier developer shall—

(A) conspicuously publish on a publicly available website of such developer a high-level summary of the audit findings and a copy of the report with appropriate redactions; and

(B) transmit a copy of the redacted report to the Under Secretary, the Attorney General, and opted-in State Attorneys General.

(5) ACCESS BY UNDER SECRETARY AND ATTORNEY GENERAL.—A large frontier developer shall grant the Under Secretary and the Attorney General

access to the third party's report, redacted consistent with subsection (f) of section 4, upon request.

(d) TRANSPARENCY REPORT.—

(1) IN GENERAL.—Before, or concurrently with, deploying a frontier model that is new or includes a substantial modification, the frontier developer of such model shall publish on a publicly available website of such developer a report on such model that includes information relating to the following:

(A) A mechanism through which an individual may communicate with such developer.

(B) The release date of such model or substantial modification.

(C) Each language supported by such model, if any.

(D) Each output modality of such model.

(E) The intended utilization of such model.

(F) Generally applicable restrictions or conditions, if any, with respect to such model.

(G) Any substantial modification to such model.

(H) Each assessment of catastrophic risk with respect to such model or substantial modification, conducted pursuant to the frontier AI framework at issue.

(I) The results of each such assessment.

(J) The extent to which a third party was utilized in the assessment of such model.

(K) Any other step taken pursuant to such framework with respect to such model.

(2) MACHINE-READABLE FORMAT.—The summaries described in this subsection shall be provided in a machine-readable format to facilitate verification of model claims.

(3) CONFIDENTIAL DEPLOYMENT.—A frontier developer may defer publication of the report required under this subsection with respect to a deployment made subject to confidentiality obligations for reasons of security or national security, until such model is first deployed other than subject to such obligations, if such developer transmits such report to the Under Secretary before or concurrently with the confidential deployment.

(e) FALSE OR MISLEADING STATEMENTS.—

(1) IN GENERAL.—Except as provided in paragraph (2), a frontier developer may not in a report under subsection (d) knowingly make an inaccurate statement about, or convey a false impression re-

garding, any subject on which subsection (d) requires such report to include information.

(2) EXCEPTION.—Paragraph (1) does not apply to a statement a frontier developer made in good faith and that was reasonable under the circumstances.

(f) REDACTIONS.—

(1) IN GENERAL.—Before publishing a report or other information pursuant to this section, a frontier developer may make a redaction in such publication to carry out any of the following:

(A) Protect a trade secret, the risk-prevention mechanisms, or the cybersecurity, of such developer.

(B) Protect public safety or the national security of the United States.

(C) Comply with Federal or State law.

(2) JUSTIFICATION.—If a frontier developer makes a redaction pursuant to paragraph (1), such developer shall carry out the following:

(A) Include in the publication in which such redaction is made information relating to the character of such redaction and a justification for such redaction.

(B) Retain for not less than five years from the date of such publication the information so redacted.

(C) Transmit to the Under Secretary an unredacted copy of the publication in which such redaction is made.

(g) REPORTING MECHANISMS.—

(1) CRITICAL SAFETY INCIDENTS.—Not later than 180 days after the date of enactment of this Act, the Under Secretary shall establish a mechanism for a frontier developer or member of the public to confidentially carry out the following:

(A) Submit to the Under Secretary a report on a critical safety incident that includes the following:

(i) A specification of the date of such incident.

(ii) Information relating to such incident, including—

(I) the reason why such incident is a critical safety incident; and

(II) whether such incident is associated with the internal utilization of a frontier model.

(iii) Any additional information required by the Under Secretary by regulation.

(B) Amend such report, as necessary.

(2) CATASTROPHIC RISK.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Under Secretary shall establish a mechanism for a large frontier developer to confidentially submit to the Under Secretary a report on catastrophic risk arising from a frontier model of such developer, including internal use and internally deployed models.

(B) PERIODIC TRANSMITTAL.—Not less frequently than every 3 months, or pursuant to another reasonable schedule specified by a large frontier developer in writing and agreed to by the Under Secretary, such developer shall transmit to the Under Secretary, through the mechanism established under subparagraph (g)(2)(A), a summary of an assessment of catastrophic risks arising from internal use of its frontier models.

(3) PROTECTION OF REPORTS.—The Under Secretary shall take all necessary precautions to

limit access to any reports submitted under this subsection to only personnel with a specific need to know the information and to protect the reports from unauthorized access.

(4) REVIEW.—The Under Secretary shall review each report submitted under this subsection by a frontier developer and may review any report submitted under this subsection by a member of the public.

(h) DISCOVERY OF A CRITICAL SAFETY INCIDENT.—

(1) IN GENERAL.—Subject to subsection (g) and except as provided in paragraph (2), not later than 72 hours after a frontier developer learns facts sufficient to establish a reasonable belief that a critical safety incident has occurred with respect to a frontier model of such developer, such developer shall submit through the mechanism established under subsection (g)(1) a report on such incident.

(2) IMMINENT RISK.—Not later than 24 hours after a frontier developer discovers a critical safety incident that poses an imminent risk of death or serious physical injury, such developer shall report such incident to a law enforcement agency with jurisdiction over such incident.

(i) STATE ATTORNEYS GENERAL OPT-IN.—Pursuant to the regulations promulgated by the Under Secretary under section 3, State Attorneys General may opt in to receive reports submitted to the Under Secretary under subsections (g) and (h).

(j) CIVIL PENALTY.—

(1) IN GENERAL.—A frontier developer that violates this section shall be subject to a civil penalty of not more than $1,000,000 per violation. For purposes of this paragraph, each day during which a violation continues constitutes a separate violation.

(2) ACTION BY ATTORNEY GENERAL.—The Attorney General may bring an action to collect a civil penalty under paragraph (1) and for an injunction ensuring compliance with the provisions of this section.

(3) ACTION BY STATE ATTORNEY GENERAL.—

(A) A State Attorney General who has opted in under subsection (i) may bring an action to collect a civil penalty under paragraph (1) and for an injunction ensuring compliance with the provisions of this section.

(B) Before filing an action under subparagraph (A), the State Attorney General shall provide to the Attorney General and the Under

Secretary a written notice of that action and a copy of the complaint for that action. This notice requirement shall not apply if the State Attorney General determines that it is not feasible to provide notice before the filing of the action, in which case the State Attorney General shall provide a written notice of the action and a copy of the complaint for the action at the same time the State Attorney General files the action.

(C) Upon receiving notice under subparagraph (B), the Attorney General shall have the right to intervene in the action that is the subject of the notice, in which case the Attorney General shall have the right to be heard with respect to any matter that arises in that action and to file a petition for appeal.

(D) In any case in which an action is instituted by the Attorney General under subparagraph (A), no State Attorney General may, during the pendency of that action, institute an action under this subsection against any defendant named in the complaint in that action for any violation asserted in the Attorney General's action.

(E) If, after a State Attorney General institutes an action under this subsection, the Attorney General institutes an action with respect to violations at issue in the State Attorney General's action, the State Attorney General's action shall be stayed as to the violations at issue in the Attorney General's action during the pendency of the Attorney General's action. If the Attorney General's action is dismissed with respect to any of the violations at issue in the State Attorney General's action without a binding resolution on the merits, the stay of the State Attorney General's action shall be lifted as to those violations.

(k) REGISTRATION AND DISCLOSURE.—

(1) IN GENERAL.—Beginning on the date that is 1 year after the date of enactment of this Act, or 90 days after a developer first qualifies as a large frontier developer, whichever is later, a large frontier developer may not develop, deploy, or operate a frontier model, in whole or in part, without a current disclosure statement filed with the Under Secretary and payment of the fee required under subsection (k)(4).

(2) CONTENTS.—A disclosure statement filed under subsection (k)(1) shall be in the form and manner prescribed by the Under Secretary and shall identify—

(A) the identity of the large frontier developer and all names under which it conducts business;

(B) the address of the large frontier developer's principal place of business and each office it maintains in the United States;

(C) in the case of a large frontier developer that is privately or closely held, or whose ultimate parent is privately or closely held, all persons or entities that beneficially own a 5 percent or greater interest in such developer at the time of filing, and all persons that formerly beneficially owned a 5 percent or greater interest in such developer or a predecessor of such developer during the preceding 5 years, and, in the case of a large frontier developer that is publicly traded, or whose ultimate parent is publicly traded, all persons or entities that beneficially own a 50 percent or greater interest in such developer at the time of filing; and

(D) the name and contact information of a primary, secondary, and tertiary point of contact, the primary of whom is responsible for receiving inquiries under this Act.

(3) RENEWAL.—A large frontier developer shall renew its disclosure statement annually, or not later than the date of any transfer of ownership of a frontier model or material change to the information reported under paragraph (k)(2), whichever occurs earlier.

(4) FEES.—The Under Secretary shall charge and collect fees from large frontier developers sufficient to offset the expenses of administering this subsection.

(5) PUBLICATION.—The Under Secretary shall maintain and publish a list of large frontier developers that have filed a disclosure statement under this subsection, excluding the contact information described in paragraph (k)(2).

(6) CIVIL PENALTY.—A large frontier developer that develops, deploys, or operates a frontier model without a current disclosure statement on file under this subsection, that submits false information in such a statement, or that fails to timely pay a fee required under paragraph (k)(4), shall be subject to

a civil penalty of $10,000 for each day of noncompliance, which the Attorney General or a State Attorney General who has opted in under subsection (i) may bring an action to collect.

(l) UNDER SECRETARY REPORTS.—Not later than January 1, 2028, and annually thereafter, the Under Secretary shall submit to Congress and the President a report that includes, for the annual period covered by such report, anonymized and aggregated information about the critical safety incidents, if any, that have been reviewed by the Under Secretary pursuant to subsection (g)(4), excluding any information that would compromise a trade secret, risk-prevention mechanisms, or the cybersecurity of a frontier developer, public safety, or the national security of the United States.

SEC. 5. INDEPENDENT VERIFICATION.

(a) LICENSING AND OVERSIGHT OF IVOS.—The Under Secretary shall have the power and duty to oversee the licensing of independent verification organizations, in accordance with the regulations prescribed under subsection (c) of section 3.

(b) ASSESSMENT REQUIREMENT.—Not later than one year after the date on which the Under Secretary first licenses an IVO with capacity to accept an engagement under this section, or 90 days after a developer first qualifies as a very large frontier developer, whichever is later, a very large frontier developer shall retain an independent verification organization that has been licensed pursuant to the regulations prescribed under subsection (c) of section 3 to perform ongoing assessment of the adequacy of the very large frontier developer's frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks for achieving acceptable levels of catastrophic risk mitigation. All assessment, monitoring, reporting, and corrective action obligations under this section shall apply to catastrophic risks arising from a very large frontier developer's internal use of frontier models, in addition to catastrophic risks arising from the release of such frontier models for use by third parties.

(c) LICENSING.—Each person or entity seeking to act as an IVO shall obtain a license from the Under Secretary.

(d) SUBCONTRACTING.—

(1) IN GENERAL.—An IVO may subcontract one or more portions of an assessment to an organization with specialized expertise, provided that the retaining IVO remains fully responsible for the assessment, any resulting assessment report, and any other regulatory obligations of the IVO under this Act.

(2) PASS-THROUGH OF OBLIGATIONS.—A subcontractor performing any portion of an assessment shall stand in the place of the retaining IVO and shall be subject to, and comply with, every obligation under this section and the regulations prescribed under subsection (c) of section 3 that applies to the IVO with respect to the work the subcontractor performs, including the personnel technical-qualification, conflict-of-interest, and confidentiality requirements.

(3) RESPONSIBILITY OF RETAINING IVO.—Notwithstanding any subcontracting under this subsection, the retaining IVO shall remain the responsible party for the assessment and the resulting assessment report, including the certifications required under subsection (f).

(e) ACCESS.—

(1) IN GENERAL.—A very large frontier developer shall grant an IVO timely access upon request to unredacted materials, records, personnel, systems, and all other information reasonably necessary for conducting the assessments and ongoing monitoring required by this section.

(2) SECURITY PROTOCOLS.—A very large frontier developer may impose reasonable security proto-

cols and confidentiality requirements upon IVOs that are narrowly tailored to protect trade secrets and confidential business information.

(3) LIMITATIONS DESCRIBED.—Any material limitation on scope, access, or information available to the IVO shall be described in the assessment report.

(f) ASSESSMENT REPORTS.—

(1) FREQUENCY.—A licensed IVO retained under subsection (b) shall determine, in its professional judgment and consistent with any regulations issued under subsection (c) of section 3, the frequency with which it prepares and submits assessment reports under this subsection, based on the nature, severity, and evolution of the catastrophic risks presented by the very large frontier developer's development, deployment, and internal use of frontier models, provided that the IVO shall prepare and submit an assessment report not less frequently than once every 6 months.

(2) CONTENTS.—Each assessment report shall be submitted simultaneously to the Under Secretary and the very large frontier developer and shall include all of the following:

(A) A description of the scope of the assessment, the time period covered, the materials reviewed, and the methods used.

(B) A description of any limitations on the IVO's ability to thoroughly and adequately assess the adequacy of the very large frontier developer's frontier AI framework.

(C) A detailed assessment of the adequacy of the very large frontier developer's frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks to ensure acceptable levels of catastrophic risk mitigation.

(D) Any identified failure, deficiency, or material weakness in achieving acceptable levels of catastrophic risk mitigation.

(E) Any corrective actions recommended to the very large frontier developer's frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks, necessary to achieve acceptable levels of catastrophic risk mitigation.

(F) The signature of the IVO's lead assessment partner or equivalent responsible official certifying that—

(i) the report is accurate and does not omit any material information;

(ii) the IVO was qualified to conduct the assessment;

(iii) the IVO is free from conflicts of interest, as defined by regulations issued under this Act; and

(iv) the assessment complied with regulations adopted pursuant to subsection (c) of section 3.

(G) Any other materials required by rules issued pursuant to subsection (c) of section 3.

(g) POST-ASSESSMENT REPORT.—

(1) Not later than fourteen days after the very large frontier developer's receipt of an assessment report under subsection (f), the very large frontier developer shall submit to the IVO a written description of the actions that it has taken or intends to take to implement the corrective actions recommended in such assessment report.

(2) Not later than seven days after receiving the description under paragraph (1), the IVO shall submit to the very large frontier developer an opinion, signed by the IVO's lead assessment partner or equivalent responsible official, stating the IVO's pro-

fessional judgment regarding whether the actions the very large frontier developer has taken or intends to take in response to the IVO's recommendations are adequate to ensure acceptable levels of catastrophic risk mitigation.

(3) Not later than 30 days after the very large frontier developer's receipt of an assessment report under subsection (f), a very large frontier developer shall submit to the Under Secretary a post-assessment report, which shall include—

(A) a copy of the frontier AI framework applicable to the assessed period;

(B) the name, business address, electronic mail address, and telephone number of the IVO and the lead assessment partner or equivalent responsible official;

(C) a summary of the key findings of the assessment, including—

(i) the IVO's determination regarding the developer's conformance with its frontier AI framework;

(ii) any significant concerns identified by the IVO regarding the adequacy of the frontier AI framework and the developer's conformance to its frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks, to ensure acceptable levels of catastrophic risk mitigation; and

(iii) the opinion rendered by the IVO under paragraph (2); and

(D) such additional information as the Under Secretary may require by regulation.

(h) AD HOC ASSESSMENTS.—At any time, and without regard to any frequency determined under paragraph (f)(1), the Under Secretary may require a very large frontier developer to obtain an ad hoc assessment, or a licensed IVO to prepare and submit an assessment report, as the Under Secretary determines necessary to—

(1) reproduce or validate assessment findings;

(2) evaluate implementation of corrective actions recommended under paragraph (f)(2)(E); or

(3) monitor significant changes in risk, including after a critical safety incident or a substantial modification to a very large frontier developer's model, system, or operations.

(i) OUT-OF-CYCLE ASSESSMENT AND REPORTING.—In addition to the assessment reports required under subsection (f), a licensed IVO shall prepare and submit simultaneously to the Under Secretary and the very large frontier developer supplemental reports as specified in this subsection.

(1) TRIGGERING DETERMINATIONS.—An IVO shall submit a supplemental report not later than seven days after the IVO determines, in light of new information, emergent model capabilities, or material changes to a frontier model, that—

(A) a prior assessment report's finding that a very large frontier developer is achieving acceptable levels of catastrophic risk mitigation is no longer valid;

(B) corrective actions recommended in a prior assessment report would no longer be adequate to achieve acceptable levels of catastrophic risk mitigation; or

(C) any representation made by a very large frontier developer in a prior post-assessment report submitted under subsection (g) is no longer accurate or is materially misleading.

(2) CONTENTS.—A report submitted under this subsection shall include—

(A) a detailed description of the information and conclusions triggering reporting under paragraph (1);

(B) an assessment of whether the issue triggering reporting under paragraph (1) threatens an imminent catastrophic risk; and

(C) any additional corrective actions or modifications to the developer's frontier AI framework, governance policies and practices, risk-monitoring, and mitigation of detected risks necessary to restore acceptable levels of catastrophic risk mitigation.

(3) DEVELOPER RESPONSE.—Not later than seven days after the very large frontier developer's receipt of a supplemental report under this subsection, the very large frontier developer shall submit to the IVO a written description of the actions that it has taken or intends to take to implement the corrective actions recommended in such supplemental report.

(4) IVO OPINION.—Not later than seven days after receiving the description under paragraph (3), the IVO shall submit to the very large frontier developer an opinion, signed by the IVO's lead assessment partner or equivalent responsible official, stating the IVO's professional judgment regarding whether the actions the very large frontier developer has taken or intends to take in response to the

IVO's recommendations are adequate to ensure acceptable levels of catastrophic risk mitigation.

(5) SUBMISSION TO UNDER SECRETARY.—Not later than twenty-one days after the very large frontier developer's receipt of a supplemental report under this subsection, the very large frontier developer shall submit to the Under Secretary—

(A) a response identifying any actions, including revisions to the frontier AI framework, that the developer has taken or intends to take in response; and

(B) an opinion rendered by the IVO under paragraph (4).

(j) PUBLIC DISCLOSURE OF ASSESSMENT REPORTS.—

(1) IN GENERAL.—Not later than 30 days after receiving an assessment report under subsection (f), a very large frontier developer shall—

(A) conspicuously publish on a publicly available website of such developer a high-level summary of the findings of such report and a copy of such report, redacted consistent with subsection (m); and

(B) transmit a copy of the report, as so redacted, to the Under Secretary, the Attorney General, and opted-in State Attorneys General.

(2) REDACTION DISPUTES.—If the Under Secretary, the Attorney General, or a State Attorney General who has opted in under subsection (k) determines that a redaction made under this subsection is overbroad, such official may request that the Under Secretary review the redaction. Not later than 30 days after receiving such a request, the Under Secretary shall review the redaction, which review may include an in camera review of the unredacted assessment report, and shall determine whether the redaction is consistent with subsection (m).

(k) STATE ATTORNEYS GENERAL OPT-IN.—Pursuant to the regulations promulgated by the Under Secretary under section 3, State Attorneys General may opt in to receive reports pursuant to subsections (f) and (i) and referrals pursuant to subsection (p).

(l) RECORDKEEPING.—Each very large frontier developer and IVO shall retain an unredacted copy of each assessment report and materials supporting the report for not less than 5 years after the date of completion of the assessment.

(m) PUBLIC VERSION REDACTIONS.—

(1) PERMITTED REDACTIONS.—The public version of an assessment report may redact information, or omit information included in a confidential annex, only to the extent reasonably necessary to protect—

(A) trade secrets;

(B) cybersecurity;

(C) a frontier developer's risk-prevention mechanisms;

(D) public safety;

(E) national security; or

(F) personally identifiable information or other information the disclosure of which would constitute a clearly unwarranted invasion of privacy.

(2) DESCRIPTION OF REDACTIONS.—The public version of the assessment report shall include a description of the character and justification of any redactions or omitted material.

(n) ACCESS TO UNREDACTED MATERIALS.—The developer and IVO shall provide the Under Secretary and the Attorney General access to the unredacted assessment report and supporting materials upon request.

(o) PROHIBITION ON MISREPRESENTATION.—An IVO shall not knowingly make a material misrepresentation or omission in any report or opinion prepared pursuant to this section.

(p) ENFORCEMENT.—

(1) REFERRAL TO ATTORNEY GENERAL AND STATE ATTORNEYS GENERAL.—

(A) IN GENERAL.—An IVO may refer any violation of this section to the Attorney General, and all State Attorneys General opting in under subsection (k), for enforcement action under this subsection.

(B) IVO REFERRALS.—If, in the course of performing its responsibilities under this section, an IVO determines that a very large frontier developer's frontier model fails to achieve acceptable levels of catastrophic risk mitigation in a manner that poses an imminent catastrophic risk, the IVO shall refer the matter to the Secretary, for consideration of an emergency order under section 8, as soon as practicable, and in any event not more than 72 hours, after its determination.

(2) DEVELOPER VIOLATIONS.—

(A) IN GENERAL.—A very large frontier developer that violates subsection (b), (e), (g), (h), (i), (j), or (k), or that makes a material misrepresentation or omission in a post-assessment report submitted under subsection (g), shall be subject to a civil penalty of not more than $1,000,000 per violation. For purposes of this subparagraph, each day during which a violation continues constitutes a separate violation.

(B) ACTION BY ATTORNEY GENERAL.—The Attorney General may bring an action to collect a civil penalty under subparagraph (A) and for an injunction ensuring compliance with the provisions of this section.

(C) ACTION BY STATE ATTORNEY GENERAL.—

(i) A State Attorney General who has opted in under subsection (k) may bring an action to collect a civil penalty under subparagraph (A) and for an injunction ensuring compliance with the provisions of this section.

(ii) Before filing an action under clause (i), the State Attorney General shall provide to the Attorney General a written notice of that action and a copy of the complaint for that action. This notice requirement shall not apply if the State Attorney General determines that it is not feasible to provide notice before the filing of the action, in which case the State Attorney General shall provide a written notice of the action and a copy of the complaint for the action at the same time the State Attorney General files the action.

(iii) Upon receiving notice under clause (ii), the Attorney General shall have the right to intervene in the action that is the subject of the notice, in which case the Attorney General shall have the right to be heard with respect to any matter that arises in that action and to file a petition for appeal.

(iv) In any case in which an action is instituted by the Attorney General under subparagraph (B), no State Attorney General may, during the pendency of that action, institute an action under this subparagraph against any defendant named in the complaint in that action for any violation asserted in the Attorney General's action.

(v) If, after a State Attorney General institutes an action under this subparagraph, the Attorney General institutes an action under subparagraph (B) with respect to violations at issue in the State Attorney General's action, the State Attorney General's action shall be stayed as to the violations at issue in the Attorney General's action during the pendency of the Attorney General's action. If the Attorney General's action is dismissed with respect to any of the violations at issue in the State Attorney General's action without a binding resolution on the merits, the stay of the State Attorney General's action shall be lifted as to those violations.

(q) IMMUNITY FROM SUIT.—

(1) IN GENERAL.—An IVO shall be immune from suit and liability under Federal and State law with respect to all claims for loss caused by, arising out of, relating to, or resulting from the materialization of a catastrophic risk of a frontier model assessed by the IVO if the IVO was licensed by the

Under Secretary under this section at the time of the assessment.

(2) EXCEPTION.—The sole exception to immunity from suit and liability of a licensed IVO under this subsection shall be an exclusive Federal cause of action for death or serious physical injury proximately caused by willful misconduct, as defined by section 247d-6d(c)(1) of title 42, United States Code.

(A) An action under this paragraph may be brought for wrongful death or serious physical injury by any person who suffers such injury or by any representative of such a person.

(B) In an action under this paragraph, the plaintiff shall have the burden of proving by clear and convincing evidence willful misconduct by the IVO and that such willful misconduct caused death or serious physical injury. Notwithstanding any other provision of law, an IVO shall not have engaged in willful misconduct as a matter of law where such IVO acted consistent with its obligations under this section and all applicable regulations, guidelines, or recommendations by the Under Secretary.

(C) An action under this paragraph shall be filed and maintained only in an appropriate district court of the United States. The substantive law for decision in such an action shall be derived from the law, including choice-of-law principles, of the State in which the alleged willful misconduct occurred, unless such law is inconsistent with or preempted by Federal law, including provisions of this section.

(D) In an action under this paragraph, no discovery shall be allowed before the IVO has had a reasonable opportunity to file a motion to dismiss, or, in the event such a motion is filed, before the court has ruled on such motion.

(r) FOIA EXEMPTION.—Assessment reports, summaries, and supporting materials disclosed to the Under Secretary pursuant to this section are exempt from disclosure under section 552 of title 5, United States Code.

SEC. 6. CUMULATIVE OBLIGATIONS.

Except as otherwise expressly provided, a large frontier developer shall comply with each requirement of this Act applicable to a frontier developer, and a very large frontier developer shall comply with each requirement of this Act applicable to a frontier developer and to a large frontier developer.

SEC. 7. GOVERNMENT ACCOUNTABILITY OFFICE REPORT ON THE MARKET FOR INDEPENDENT VERIFICATION ORGANIZATIONS.

(a) ANNUAL REPORT.—Not later than one year after the date of enactment of this Act, and annually thereafter, the Comptroller General of the United States shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report on the state of the market for independent verification organizations licensed under section 5.

(b) CONTENTS.—Each report submitted under subsection (a) shall include the following:

(1) An assessment of the state of the market for independent verification organizations, including the number of licensed IVOs, their capacity to meet demand for assessments, and any barriers to entry or other factors affecting the development of a competitive and robust IVO market.

(2) An evaluation of the degree to which independent verification organizations are independent from the artificial intelligence industry, including any factors that threaten such independence.

(3) Recommendations for legislative or administrative policy changes that would help ensure the

independence of independent verification organizations from the artificial intelligence industry.

SEC. 8. EMERGENCY ORDERS ADDRESSING IMMINENT CATASTROPHIC RISK.

(a) AUTHORITY.—

(1) IN GENERAL.—The Secretary may issue an emergency order suspending or restricting a frontier developer's development, deployment, or internal use of a frontier model upon finding that such development, deployment, or internal use of that model presents an imminent catastrophic risk.

(2) EMERGENCY ORDER.—In this section, the term "emergency order" means a provisional order issued under subsection (e) or a final order issued under subsection (f).

(3) SCOPE.—A suspension or restriction under this section—

(A) may apply to the whole or any part of the development, deployment, or internal use of the frontier model, including development, deployment, or internal use by or with respect to particular persons or categories of persons, for particular purposes or uses, or through particular means or channels of access; and

(B) may be defined by reference to the presence or absence of specified facts or circumstances of such development, deployment, or internal use, including specified safeguards or security measures.

(b) FINDING.—

(1) IN WRITING.—A finding under subsection (a) shall be set forth in a written statement that includes the factual basis for the finding and the principal reasons for the Secretary's determination.

(2) TECHNICAL ASSESSMENT.—If the Secretary has published methods bearing on the finding, the Secretary shall, before the Secretary makes the finding, prepare a technical assessment applying such methods to the frontier developer's development, deployment, or internal use, and the Secretary shall include such assessment with the written statement under paragraph (1).

(3) CONSULTATION.—In making a finding under subsection (a), a preliminary determination under subsection (e), or a determination with respect to rescission under subsection (g), the Secretary shall consult with the Under Secretary.

(4) FINAL AUTHORITY.—The authority to make a finding under subsection (a) and to issue, renew,

or rescind an emergency order under this section is vested in the Secretary, and no consultation under paragraph (3) shall be construed to condition the exercise of such authority on the concurrence of the Under Secretary.

(c) ORDER.—

(1) CONTENTS.—An emergency order shall—

(A) identify the frontier developer subject to the order and the frontier model or models to which the order applies;

(B) describe, with reasonable particularity, the acts, practices, or circumstances in the development, deployment, or internal use of such model or models from which the imminent catastrophic risk arises;

(C) state, in the case of a provisional order, the preliminary basis for the order, and in the case of a final order, include the written statement required by subsection (b)(1);

(D) describe the suspensions or restrictions imposed;

(E) include a timeline for compliance with the order;

(F) state the criteria for rescission of the order under subsection (g); and

(G) if corrective action by the frontier developer could cause such development, deployment, or internal use to no longer present an imminent catastrophic risk, describe such corrective action.

(2) RULE OF CONSTRUCTION.—The identification or availability of corrective action described in paragraph (1)(G) shall not be a precondition to the issuance of an emergency order.

(d) EFFECTIVENESS AND APPLICATION.—

(1) EFFECTIVENESS.—An emergency order is effective upon service on the frontier developer and, unless set aside, limited, or suspended under subsection (j) or subsection (k), remains effective and enforceable until it lapses under subsection (e)(3) or subsection (f)(2) or is rescinded under subsection (g).

(2) PERSONS BOUND.—An emergency order binds the frontier developer subject to the order, each affiliate of such developer, and the successors and assigns of such developer and its affiliates, and any other person who, with actual notice of the order, acts in concert or participation with such developer, affiliate, successor, or assignee in the devel-

opment, deployment, or internal use suspended or restricted by the order.

(3) MODIFIED AND DERIVED MODELS.—

(A) MODIFIED MODELS.—Unless the order provides otherwise, an emergency order applies to any model produced by modification of the weights or parameters of a frontier model identified in the order under subsection (c)(1), including by fine-tuning, reinforcement learning, quantization, pruning, or merging with another model.

(B) DERIVED MODELS.—Unless the order provides otherwise, an emergency order also applies to any model developed after service of the order that is trained, in substantial part, on the outputs, weights, or internal representations of a frontier model identified in the order.

(C) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to limit the authority of the Secretary to identify a model in an emergency order under subsection (c)(1), or by amendment to such order.

(e) PROVISIONAL ORDERS.—

(1) IN GENERAL.—Notwithstanding subsection (a)(1), the Secretary may issue a provisional order

before making the finding required by subsection (a), upon a preliminary determination that the frontier developer's development, deployment, or internal use of a frontier model presents an imminent catastrophic risk. A provisional order may be issued whether or not a technical assessment under subsection (b)(2) has been prepared.

(2) NOTICE AND OPPORTUNITY TO CURE.—Before issuing a provisional order, the Secretary shall provide the frontier developer notice and an opportunity to cure and to be heard, unless the Secretary determines that the imminence of the catastrophic risk forecloses such notice and opportunity, in which case the Secretary shall set forth such determination, and the basis therefor, in writing, and serve such determination with the provisional order.

(3) LAPSE.—

(A) IN GENERAL.—A provisional order shall lapse upon the earliest of—

(i) the date that is 45 days after the date of service of the order on the frontier developer;

(ii) if the frontier developer has timely applied for an expedited hearing under subsection (j)(1), the date that is 7 days after the date on which the Secretary renders a final determination on such application; or

(iii) the date on which a final order is issued under subsection (f) suspending or restricting the same or substantially similar development, deployment, or internal use.

(B) ORDERS ISSUED WITHOUT NOTICE.—If a provisional order is issued without notice and an opportunity to cure pursuant to a determination under paragraph (2), the Secretary shall, promptly after service of the order, provide the frontier developer an opportunity to cure, and subparagraph (A) shall apply to the order.

(4) SUCCESSIVE PROVISIONAL ORDERS.—The Secretary may not issue a provisional order to a frontier developer suspending or restricting the same or substantially similar development, deployment, or internal use as a prior provisional order, except on the basis of facts and circumstances materially different from those on which the prior provisional order rested.

(f) FINAL ORDERS.—

(1) IN GENERAL.—The Secretary may issue a final order if—

(A) a provisional order suspending or restricting the same or substantially similar development, deployment, or internal use is in effect at the time the Secretary issues the final order;

(B) the Secretary has made the finding required by subsection (a), set forth in the written statement required by subsection (b)(1); and

(C) either—

(i) the period to apply for an expedited hearing under subsection (j)(1) has lapsed without an application; or

(ii) the Secretary has rendered a final determination on an application under subsection (j)(1).

(2) LAPSE.—A final order shall lapse upon the date that is 90 days after the date on which it is issued.

(3) RENEWAL.—The Secretary may renew a final order for one or more successive periods of not more than 90 days each if, before the order lapses, the Secretary makes a new finding under subsection (a), in accordance with subsection (b), based on the

facts as they exist at the time of renewal. A renewal shall be treated as a final order for purposes of subsection (k).

(g) RESCISSION.—

(1) REQUIRED RESCISSION.—The Secretary shall rescind an emergency order, in whole or in part, if—

(A) the criteria for rescission stated in the order under subsection (c)(1) are satisfied; or

(B) the development, deployment, or internal use suspended or restricted by the order would not present an imminent catastrophic risk if the order were rescinded to that extent.

(2) WRITTEN DETERMINATION.—A rescission under this subsection, and any denial of an application under paragraph (3), shall be set forth in a written determination stating the basis therefor, which shall be served on the frontier developer.

(3) APPLICATION.—A frontier developer subject to an emergency order may apply to the Secretary for rescission of the order in whole or in part. The Secretary shall grant or deny the application not later than 14 days after its receipt.

(4) SUCCESSIVE APPLICATIONS.—Following the denial of an application under paragraph (3), the

Secretary may summarily deny a subsequent application respecting the same order that does not rest, in substantial part, on facts or circumstances arising after, or not reasonably available at the time of, the prior application.

(h) PUBLICATION.—

(1) IN GENERAL.—The Secretary shall publish each final order issued under subsection (f), each renewal of a final order under subsection (f)(3), and each written determination under subsection (g)(2) rescinding an order in whole or in part, subject to paragraph (2).

(2) REDACTIONS.—Before publishing an order, renewal, or rescission under paragraph (1), the Secretary may make a redaction in such publication to protect a trade secret, risk-prevention mechanisms, or the cybersecurity, of the frontier developer, to protect public safety or the national security of the United States, or to comply with Federal or State law. If the Secretary makes such a redaction, the Secretary shall include in the publication information relating to the character of, and a justification for, such redaction.

(i) CONGRESSIONAL NOTIFICATION.—

(1) NOTICE OF ORDERS.—Not later than 3 days after issuing an emergency order, or renewing a final order under subsection (f)(3), the Secretary shall submit to the appropriate congressional committees—

(A) a copy of the order;

(B) in the case of a final order or renewal, the written statement required by subsection (b)(1), and in the case of a provisional order, a statement of the preliminary basis for the order;

(C) any technical assessment prepared under subsection (b)(2); and

(D) in the case of a provisional order issued without notice and an opportunity to cure, the Secretary's written determination under subsection (e)(2).

(2) NOTICE OF DISPOSITION.—Not later than 7 days after an emergency order is rescinded, lapses, or is set aside, limited, suspended, or stayed in whole or in part by the Secretary or a court, the Secretary shall notify the appropriate congressional committees of such disposition and its basis.

(3) FORM.—Each submission under this subsection shall be in unclassified form to the maximum

extent practicable, but may include a classified annex.

(4) PERIODIC REPORT.—Not less frequently than semiannually, the Secretary shall submit to the appropriate congressional committees a report on the exercise of authority under this section, including each order issued, renewed, rescinded, or lapsed during the period; the outcome of each hearing under subsection (j) and each action or proceeding under subsection (k), subsection (l)(3), and subsection (m); and any changes to the methods published by the Secretary bearing on findings under this section.

(5) DEFINITION.—In this subsection, the term ''appropriate congressional committees'' means the Committee on Commerce, Science, and Transportation of the Senate, the Committee on Energy and Commerce of the House of Representatives, and the Committee on the Judiciary of each House of Congress.

(j) ADMINISTRATIVE REVIEW.—

(1) EXPEDITED HEARING.—Not later than 10 days after the date on which a provisional order is served on a frontier developer, the frontier developer may apply for an expedited hearing on such order.

The Secretary shall hold such hearing and render a final determination on such application not later than 30 days after the application's receipt. The hearing may be conducted by a hearing officer designated by the Secretary.

(2) RECORD ACCESS AND BURDEN.—In a hearing under paragraph (1), the Secretary shall make available to the frontier developer any written determination under paragraph (e)(2), any technical assessment under paragraph (b)(2), and all information on which the Secretary relied in issuing the order, and shall bear the burden of demonstrating that adequate evidence supports the order.

(k) JUDICIAL REVIEW.—

(1) REVIEW OF PROVISIONAL ORDERS.—A provisional order shall not be deemed final agency action for purposes of section 704 of title 5, United States Code. Except as provided in paragraph (7), no court shall have jurisdiction to review, enjoin, set aside, suspend, limit, or stay a provisional order before a final order has been issued under subsection (f); thereafter, the lawfulness of the provisional order may be reviewed only in a proceeding under paragraph (2).

(2) EXCLUSIVE JURISDICTION AND EXPEDITION.—Notwithstanding any other provision of law, the United States District Court for the District of Columbia shall have exclusive jurisdiction over any civil action seeking judicial review of, or any order enjoining, setting aside, limiting, suspending, staying, or otherwise affecting the effectiveness or enforcement of, an emergency order under this section or relief under paragraph (l)(3). The court shall expedite the action to the greatest possible extent, and shall establish a schedule for the proceeding not later than 10 days after the action is filed.

(3) NO AUTOMATIC STAY.—The filing of a civil action referenced in paragraph (2) shall not operate as a stay of the emergency order unless the district court orders otherwise.

(4) STANDARD OF REVIEW.—The district court may set aside, limit, suspend, or stay a final order only if the court determines that such order is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.

(5) ENFORCEMENT PROCEEDINGS.—The validity of a final order may not be reexamined in an action under subsection (m).

(6) APPEAL.—An appeal from a final judgment of the district court in an action referenced in paragraph (2) may be taken to the United States Court of Appeals for the District of Columbia Circuit not later than 30 days after the date of the judgment. The court of appeals shall expedite the appeal to the greatest possible extent. It shall be the duty of every court of the United States to advance on the docket and to expedite the disposition of any action or appeal under this subsection.

(7) CONSTITUTIONAL CLAIMS.—Nothing in this subsection shall be construed to preclude the jurisdiction of a court of the United States over a claim that this section, or the structure or authority of the Secretary under this Act, violates the Constitution of the United States.

(l) EXCLUSIVITY.—

(1) EXCLUSIVE MEANS.—This section shall be the exclusive means by which any department, agency, officer, or employee of the United States, including the President, may take any action that has the purpose or effect of suspending, restricting, conditioning, or otherwise limiting a frontier developer's development, deployment, or internal use of a frontier model, and that is taken, in whole or in substan-

tial part, on the ground that such development, deployment, or internal use presents an imminent catastrophic risk.

(2) CONSTRUCTION.—No other provision of law shall be construed as authorizing an action described in paragraph (1), unless such provision expressly refers to this section.

(3) UNAUTHORIZED ACTIONS.—An action described in paragraph (1) that is not taken in accordance with this section shall be unenforceable, and a frontier developer against which such an action is directed may bring a civil action under paragraph (k)(2) for declaratory or injunctive relief.

(m) ENFORCEMENT.—

(1) CIVIL PENALTY.—A person bound by an emergency order under paragraph (d)(2) that violates the order shall be subject to a civil penalty of not more than $10,000,000 per violation. For purposes of this paragraph, each day during which a violation continues constitutes a separate violation.

(2) ACTION BY ATTORNEY GENERAL.—The Attorney General may bring a civil action in the United States District Court for the District of Columbia to enforce an emergency order, to collect a civil penalty under paragraph (1), or both. In such

an action, upon a showing that a person has violated, or is about to violate, an emergency order, the court shall issue an injunction, restraining order, or other order requiring compliance, without the showing of irreparable harm or the inadequacy of other remedies at law otherwise required for equitable relief.

(3) CRIMINAL PENALTY.—A person that willfully violates, or willfully directs, induces, or procures a violation of, an emergency order shall be fined not more than $1,000,000 per violation, imprisoned not more than 10 years, or both.

SEC. 9. RELATIONSHIP TO STATE LAWS.

(a) COVERED SUBJECT AREA.—For purposes of this section, the term ''Covered Subject Area'' means any of the following:

(1) FRONTIER AI RISK TRANSPARENCY.—The disclosure by a developer, to any State, member of the public, or other person, of information regarding—

(A) the policies, procedures, frameworks, or practices used by the developer to identify, assess, manage, or mitigate catastrophic risks associated with the development, training, evaluation, or release of an AI model;

(B) the results, methodologies, benchmarks, or thresholds of testing, evaluation, or red-teaming of an AI model with respect to catastrophic risks; or

(C) the characteristics, capabilities, training, or deployment of an AI model, where the disclosure relates to the assessment, monitoring, communication, or mitigation of catastrophic risks.

(2) FRONTIER AI THIRD-PARTY AUDITING AND INDEPENDENT VERIFICATION.—The assessment, audit, evaluation, certification, attestation, or verification, by a person other than its developer, of—

(A) activities involved in the development, training, evaluation, or deployment of an AI model by such developer that relate to the identification, assessment, management, or mitigation of catastrophic risks;

(B) the policies, procedures, frameworks, or practices of such developer relating to the identification, assessment, management, or mitigation of catastrophic risks; or

(C) the compliance of such developer with any requirement relating to the development, training, evaluation, or release of an AI model, if such requirement relates to the mitigation of catastrophic risks, including any requirement that such developer obtain certification, attestation, registration, accreditation, or other approval as a condition of, or in connection with, the development, training, evaluation, or release of an AI model, or that such developer provide access to an AI model, model weights, training data, source code, evaluation results, or other technical materials for purposes of any such assessment, audit, evaluation, or verification.

(3) FRONTIER AI INCIDENT REPORTING.—The reporting by a developer to any State, agency, regulator, or other governmental entity of—

(A) safety or security incidents involving an AI model, including unauthorized access to or exfiltration of model weights, loss of control over a deployed model, use of a model to cause or materially contribute to catastrophic harm, or material failure of a safety mitigation; or

(B) other events involving the development, training, evaluation, or release of an AI model that bear on the potential for the model to cause or materially contribute to catastrophic harm.

(b) PREEMPTION.—Except as provided in subsection (c), no State or political subdivision of a State may adopt or enforce any law, regulation, order, or other requirement that imposes new substantive obligations on artificial intelligence developers with respect to any Covered Subject Area.

(c) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to affect the authority of a State or political subdivision of a State to—

(1) adopt or enforce generally applicable laws, regulations, orders, or other requirements that do not target artificial intelligence developers;

(2) regulate the use or deployment of AI systems by deployers or users, including via consumer protection, civil rights, contract, criminal, or privacy laws, provided that no substantive obligations are imposed on developers with respect to model development, training, evaluation, or release;

(3) adopt or enforce laws, regulations, orders, or other requirements specifically relating to the protection of minors from harms arising from the use of AI systems, including requirements addressing sexually explicit content, content promoting self-

harm, content facilitating exploitation, age verification, parental controls, or similar matters; and

(4) adopt or enforce laws, regulations, orders, or other requirements governing the procurement or use of AI systems by State governments.

(d) DEFINITION.—In this section, the term ''artificial intelligence developer'' means—

(1) an entity that builds, designs, codes, produces, trains, or owns an artificial intelligence model or models for internal use or for use by a third party; and

(2) does not include an entity that is solely a deployer of the artificial intelligence model.