MODEL ACT

Frontier AI Public Welfare Offenses

v3.4.2 · 27 August 2026 · statutory text only ·

Contents

MODEL ACT - Frontier AI Public Welfare Offenses v3.4.2 - 27 August 2026

A model State statute placing personal, non-delegable duties on the natural persons who hold practical power over frontier computational systems deployed in or into the State, on the doctrine of United States v. Dotterweich, 320 U.S. 277 (1943), and United States v. Park, 421 U.S. 658 (1975). Failure of due care in the exercise of that authority is a misdemeanor. Knowing or willful conduct is a felony, and on conviction of it the court shall impose imprisonment unless it states on the record substantial and compelling reasons for not doing so.

Who it reaches. A natural person who holds authority over a covered system, regardless of title, regardless of whether the authority was exercised or formally vested, and regardless of whether others held it too. Delegation does not relieve that person: SEC. 4(e) provides that no appointment of a safety officer, compliance officer, committee, subsidiary or contractor shields anyone who retains the authority. Nor does resignation, removal, or disposal of the rights by which the authority was held. Nor does a want of technical expertise: SEC. 4(a) excludes professional credentials and technical ability from what constitutes authority, so that the duty attaches to the authority to decide rather than to the capacity to understand. That is Park, and it is deliberate.

WHO IT DOES NOT REACH, WHICH IS SET OUT IN ONE PLACE AT SEC. 4(b). Nobody who did not decide. Not the person who designed, built, trained, tested, evaluated, operated, or documented the system and held no authority over the decision. Not the person who raised or escalated a concern about it. Not the outside researcher who tests it in good faith, who may publish, and whom no term of access can strip of that protection. Not the person who downloads, studies, fine-tunes, or runs weights he obtained lawfully. Not the supplier of goods, services, premises, finance, or advice on ordinary commercial terms. Not a public body evaluating on its own initiative. SEC. 4(b) creates none of those exclusions; each already sits at the provision named beside it, and they are collected there because the first question asked of a criminal statute in this field is who else it catches.

WHERE IT SITS AGAINST FEDERAL PREEMPTION. Every federal instrument proposed to displace State AI law has reserved laws of general applicability and the criminal law from its operation. This Act is drafted to fall inside those reservations rather than to fight them: it licenses nothing, approves nothing, gates nothing on any officer's permission, compels no opinion, and punishes conduct of a kind this State punishes generally - endangerment by unsafe goods, unauthorized access to another's property, false statements to public officers, and the destruction of records. SEC. 13(f) states that character in the text. SEC. 13(g) then answers the other risk, which is not preemption but imitation: an enactment taking this Act's definitions, thresholds and vocabulary while omitting the natural person, the non-delegation rule, the criminal floor, the personal certification, or the records duties is not an enactment of this Act, and says so on its face.

WHAT IT DOES INSTEAD OF A FINE. The offense at SEC. 5(b) is the obtaining of unauthorized access to another's systems, data, or model weights. When a natural person obtains that access directly it is prosecuted under 18 U.S.C. § 1030 and under State computer-crime law, and people of ordinary means have gone to prison under those provisions for access causing far less harm. This Act proceeds on the view that the same access, obtained by a system a person deployed when that person had the authority to deploy it otherwise, is not answered by a payment from that person's employer. SEC. 10(c)(1)(D) sets the term for that offense at no less than what the person would face for obtaining the access directly. SEC. 10(f) provides that an entity's liability neither satisfies nor mitigates the person's, that a payment borne by the entity is not a factor in mitigation, that no deferred or declined prosecution may resolve the individual's liability without the court's approval on the record, and that no term of imprisonment may be converted to a fine.

WHAT IT MAKES CRIMINAL, AND WHAT IS ALREADY CRIMINAL FOR EVERYONE ELSE.

Offense under this Act	Already a crime for an ordinary person under
Shipping without validation	21 U.S.C. 331, 333(a)(1) — strict liability
Operating uncontrolled autonomous access that causes a breach	18 U.S.C. 1030
Failing to report	18 U.S.C. 4 — misprision, three years
Lying to the State	18 U.S.C. 1001 — five years
Destroying or withholding records	18 U.S.C. 1519 — twenty years

Read the right-hand column first. Every one of these is already a crime in the United States for an ordinary person, and most of them carry a heavier maximum sentence than this Act proposes. What this Act extends is not the criminal law. It is its reach. Each is tried to a jury when charged against an ordinary person, and each is tried to a jury under this Act; the base tier is set above six months for that reason.

ITS PENALTIES. Every act this Act makes an offense is already a crime when done by an ordinary person, and existing law punishes several of them more severely than earlier drafts of this Act did. SEC. 8 is built on the structure of 18 U.S.C. § 1350, which punishes a knowing false certification by up to ten years and a willful one by up to twenty; this Act's felony tier stood at three. That is corrected at SEC. 10(c)(1). SEC. 10(b) and SEC. 10(f) now provide that no person is punished less severely under this Act, for conduct within it, than a person owing no duty under it would be punished for the same conduct. The principle is a floor and not a ceiling: this Act does not displace the general criminal law, and SEC. 10(f) forbids treating its availability as a reason to charge the lesser offense.

SIX DECISIONS MADE, AND WHO MADE THEM. Where this Act had recorded a question as the drafter's to settle rather than counsel's, it is settled here, and the reasons are recorded in the annotated version of this Act. An evaluation run with a safeguard deliberately disabled is inside this Act, at SEC. 2(d). Commissioning an evaluation from another does not break the chain of authority, at SEC. 4(f), and an independent body evaluating on its own initiative does not create one. The deadline for the Agency to prescribe standards is mandatory and unbracketed at SEC. 3(c)(3), because the offense that matches the conduct in the record is gated on it. This Act carries no sunset, because a sunset in a criminal statute of this kind sets a date on which the duty lapses and the conduct does not. Scope reaches a model its developer has held out as frontier, at SEC. 1(b)(1). And this Act does not wait for other States, at SEC. 0(a)(13). Each of those is a choice and each can be reversed by anyone who thinks it wrong.

ON THE WORD "AI". This Act does not use it. No duty and no offense turns on whether anything is "artificial intelligence," "AI," "AGI," "machine learning," "a large language model," or an "agent." SEC. 1(b)(18) says so in terms. The term has no settled technical meaning and no measurable threshold, and a statute using it without definition covers everything and nothing. This Act reaches a class defined instead by compute, by the developer's own public description, by agency designation, and by enumerated capability tests found on the evidence. It appears in the title, and in the names of three enactments this State cannot rename. Nowhere else.

ON ITS DEFINITIONS. Seventeen terms are defined at SEC. 1(b), and six of them were added on 27 August 2026 after an audit found them carrying criminal weight while defined nowhere: what it means for a failure to materially cause a result, what "the same class of risk" means where it is the gateway to the felony tier, what a validated configuration is, what makes notice credible and starts the reporting clock, what makes a nonconformity material, and what mass-market scale is. That last had been used in an earlier draft with no figure at all, which this project's own review had already graded a defect. **A criminal statute is attacked at its vaguest term, and these were the vaguest terms.** Two remain deliberately open to the trier of fact: "materially equivalent" capabilities at SEC. 1(b)(1), and due care, which SEC. 6(a) construes against the applicable standards and the conduct of a reasonably prudent controlling person rather than defining.

ITS STATE. A research draft. It has never been introduced in any legislature and it has not been reviewed by any lawyer.

Six questions are unresolved. Each is identified below, and each is discussed at the provision it concerns in the annotated version of this Act, which states what was tried and why it failed.

SEC. 1(b) Whether capability equivalence, found on the evidence, is definite enough to carry a criminal scope term. It is the route that does not depend on the developer or on any agency, and it is the one most exposed to a vagueness challenge. SEC. 1(c) Whether this Act can reach an evaluation run outside the adopting State on a model later deployed within it. Most of the conduct that prompted this Act was of that kind, and as drafted the Act does not reach it. SEC. 0(23) Whether a validation condition on the release of model weights is a licensing scheme over publication, and so a prior restraint. Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999), so held as to encryption source code, and this Act conditions release on validation at SEC. 5(a). The subsequent history of that panel opinion has not been confirmed here and must be before it is relied on in either direction. SEC. 6(b) Whether official responsibility may supply the knowledge element of the felony tier, on which the authorities divide and this Act concedes the narrower reading; and whether that tier is available at all, given that Dotterweich and Park are misdemeanor authority. SEC. 6(g) Whether the continuing-operation provision is a genuine continuing offense or would be read as retroactivity, which is barred. SEC. 10 Whether the terms at SEC. 10(c)(1) are proportionate at the scale this Act can reach. They are taken from 18 U.S.C. § 1350, read in full on 25 August 2026, and stacking them per victim and per day may produce an aggregate no court would sustain. SEC. 10(c)(3) caps consecutive service for that reason and the cap has never been tested by anyone.

A further note, at SEC. 4(g), explains what that subsection is for rather than asking a question.

One question that stood here has been answered. It asked whether a State may presume controlling-person status in a criminal proceeding. County Court of Ulster County v. Allen, 442 U.S. 140, 157, 166-67 (1979), was read in the bound reporter on 27 August 2026: a permissive inference that allows but does not require, and places no burden on the defendant, is reviewed as applied and is not judged by the reasonable-doubt test; a mandatory presumption is. SEC. 4(c) is drafted as the first and not the second, and it stands. What remains is not a question this Act can answer on its face: whether the connection asserted at SEC. 0(a)(8) holds on the facts of a given prosecution. The asymmetry the question was really about is untouched - where the remedy is money the holder of the votes is presumed responsible and where it is prison he is not - and Allen explains that this Act may not cure it by converting the inference into a presumption.

This Act does not reach conduct completed before its commencement, and no drafting can: Article I, section 10 forbids a State to make criminal what was lawful when done. It names no person and no company; a statute that identified its defendants would be a bill of attainder under the same clause. Conduct occurring before commencement appears here as legislative findings and as admissible evidence bearing on knowledge, authority, and due care with respect to conduct that continues.

SEC. 0. FINDINGS AND PURPOSE (UNCODIFIED)

(a) The Legislature finds:

(1) Covered systems are deployed to, operated within, and made available to residents of this State, and the deaths, injuries, intrusions and losses this Act addresses occur to persons and property within this State.

(2) The protection of persons within this State from death and serious injury, and the punishment of those whose failures of care cause it, is among the oldest and most traditional exercises of this State's police power, and is the same power by which this State punishes homicide, reckless endangerment, the endangerment of the public by the sale of adulterated or unsafe goods, and false statements made to its own officers.

(3) The duties this Act imposes arise from the deployment, material expansion, release, or operation of a covered system in or into this State, or from conduct in this State in relation to such a system. This Act imposes no duty on any person by reason of research, training, or development that neither occurs in this State nor concerns a covered system deployed or released in or into this State.

(4) No provision of this Act requires any person to express, adopt, endorse, or refrain from expressing any opinion, characterization, viewpoint, or contested position, or to alter the output of any covered system. The statements this Act requires are statements of fact within the knowledge of the person making them, made to a regulator.

(5) This Act draws no distinction between persons within and persons outside this State. It confers no advantage on any in-state person and imposes no obligation on an out-of-state person that it does not impose on an in-state person engaged in the same conduct with respect to the same system.

(6) The obligations this Act imposes are, in substance, the obligations that responsible developers, providers, and deployers of covered systems already represent that they discharge, and the incremental burden of compliance is small in relation to the revenues of the persons on whom it falls.

(7) This Act supplements and does not displace the generally applicable criminal and civil law of this State, which applies to conduct concerning covered systems as it applies to all other conduct.

(8) A person holding ownership, voting, contractual, or governance rights sufficient, alone or in concert with others, to direct or replace the management of an entity ordinarily possesses, by reason of those rights, the practical power to prevent, halt, restrict, or correct a deployment by that entity, whether or not that person exercises operational supervision and whether or not the entity's internal documents assign that function to another.

(9) In the incidents known to the Legislature, the conditions that permitted a covered system to obtain unauthorized access to systems outside its operator's control were not properties of the model. They were decisions: external network access was enabled, provider security classifiers were disabled, monitoring was asynchronous or absent, the system's operating instructions were misconfigured, and the scope of the exercise was not fixed in writing. Each was a decision a natural person had authority to make differently.

(10) A monetary penalty imposed upon an entity is absorbed as a cost of doing business, is insurable in substance whatever its form, and falls upon the entity's owners rather than upon the person whose decision caused the violation. A duty that attaches personally to that person, and that cannot be insured, indemnified, or reimbursed, is the only measure the Legislature finds proportionate to the risks addressed by this Act.

(11) For each act this Act makes an offense, the general criminal law already punishes the same act when done by a person who owes no duty under this Act, and in several instances punishes it more severely: a false statement to a public officer, the destruction or falsification of a record to obstruct an investigation, the obtaining of unauthorized access to another's computer system, and the causing of death or serious injury by a failure of care. The Legislature finds that a person holding authority over a covered system should not, by reason of that authority or of the scale of the enterprise through which it is exercised, be punished less severely for that act than any other person, and this Act is not to be construed to that effect.

(12) The offense described at SEC. 5(b) is the obtaining of unauthorized access to the computer systems, data, or model weights of another. That conduct is punished, when done by a natural person acting directly, under 18 U.S.C. § 1030 and under the computer-crime law of this State, and persons of ordinary means, including students and security researchers, have been prosecuted and imprisoned under those provisions for access causing far less harm than the access this Act addresses. The Legislature finds no reason in principle why the same access, obtained by a system that a person deployed with the authority to deploy it otherwise, should be answered by a payment from that person's employer.

(13) The Legislature does not find that action by this State alone will alter the conduct of persons who owe it no duty. It finds that the duties this Act imposes fall on persons who deploy covered systems to residents of this State, that those persons are few, that they are identifiable, and that a duty owed personally by them is not discharged by relocating an entity. The Legislature further finds that the absence of an identical duty elsewhere is a reason for this State to impose one and not a reason to refrain.

(14) The Legislature notes that the federal instruments proposed to displace State law in this field have each reserved laws of general applicability and the criminal law from their operation. This Act is drafted to fall within those reservations, and SEC. 13(f) states its character for that purpose.

(15) The Legislature finds that a record may be lost without anyone destroying it. Where an organization applies an ordinary and defensible schedule for the deletion of underlying research data, the removal of a line from a report is sufficient to make the observation behind it permanently unrecoverable, and no instruction to destroy anything need be given. A records duty that attaches only to underlying data does not reach that loss, and the duty imposed by SEC. 12 attaches to the finding for that reason.

(16) The Legislature finds that the enacted law of this field already knows how to require a natural person's signature, and has required one only of the outside auditor engaged to inspect the work, and not of the person who decides that a system may be deployed. The person who signs cannot halt anything; the person who can halt it signs nothing. SEC. 8 places the signature where the authority is.

(17) The Legislature further finds that the duty to disclose a security failure presently falls upon the party intruded upon rather than upon the party whose system carried out the intrusion, and that in the incidents known to the Legislature the party broken into disclosed first and without knowing who was responsible, while the party whose system acted disclosed afterwards and at a time of its own choosing. The persons whose systems were reached were told last, through an intermediary, and no law required that they be told at all. SEC. 9(c) is directed to that finding.

(18) The Legislature notes that federal law already operates a mandatory disclosure regime for the escape of a self-replicating hazard, requiring immediate notification upon discovery and a written report within seven days, and finds no principled reason why the

escape of a system capable of acting upon the systems of others should be disclosed only at the discretion of the person who released it.

(19) The Legislature further finds that a defense founded upon conformity with a framework would have protected the wrong party in the cases known to it. Where an automated system has wrongly accused people of fraud or dishonesty, and has cost them their employment, their money, and in some cases their lives, the institution deploying it held the paper: a process, an assurance, an audited system. The paper was wrong at machine speed. A rule making the paper conclusive would have armored the accuser against the accused, and this Act declines it.

(20) The Legislature notes that another State has already required by statute that a covered employee's report of catastrophic risk be shared with the officers and directors of a large frontier developer at least quarterly, and has provided that where the report alleges wrongdoing by an officer or director it shall not be shared with that officer or director. That legislature therefore routed the warning to the officer's desk on a schedule and considered who ought not to receive it. No duty attaches on receipt. The officer is a recipient and remains one. SEC. 6(f) attaches the duty that the delivery implies.

(21) The Legislature finds that the frontier statutes enacted to date attach their duties to catastrophe rather than to conduct, on thresholds requiring deaths in the tens or damages in the billions. In the year preceding this Act, systems reached the open internet from their evaluation environments, exploited software vulnerabilities, obtained access to the systems of third parties and to data held there, and were reported by their developers as having done so. Nobody died and no such sum was lost, and it is accordingly unclear whether any existing law required that any of it be reported. A regime triggered by catastrophe is silent until catastrophe. The duties of this Act attach to conduct and to authority, and not to a count of the dead.

(22) This Act is directed at the small number of natural persons who decide that a covered system may be built, expanded, released, or kept running, and who hold the authority to decide otherwise. It is not directed at the people who do the work. The engineer who wrote the code, the researcher who ran the evaluation, the member of the safety staff who raised the concern, the contractor, the academic, the open-source contributor, the operator of a small deployment, and the ordinary user of a covered system are not the objects of this Act, and the Legislature intends that it never be construed to reach them by reason of that work. The exclusions in SEC. 4(a), the de minimis rule in SEC. 2(c), the protections in SEC. 6(f) and SEC. 11, and this finding are to be read together and given full effect for that purpose. Where the application of this Act to such a person is doubtful, the doubt is resolved against its application.

(23) The Legislature finds that a duty attaching to the release of model weights cannot require what release makes impossible, and that the persons who study, modify, and run released models are not the persons this Act is directed at. SEC. 1(b)(9) limits duties in connection with a release to those capable of performance before it; SEC. 2(d) permits the external access that safety research into external access requires; SEC. 8 does not

reach a controlled research deployment; and a person operating a released model who is neither the releasing entity nor a controlling person of it is given a period in which to comply with a suspension before any offense lies.

(24) A deployment, once begun, continues. Where a covered system remains deployed or in operation in or into this State on and after the applicable commencement under SEC. 3(c), the duties of this Act attach to its continued operation from that day forward, by reason of that continued operation and not by reason of anything done before it.

(25) The Legislature finds that responsibility for the oversight of these systems is in practice divided among the original model developer, the developer of scaffolding, the fine-tuner, the deployer offering access, and the end user, and that this division has been described by a national technical safety body, in its own published research, as leaving "no single party having sole responsibility to implement monitoring or to act on a concerning signal." The Legislature finds that a division of responsibility with that effect is the mechanism by which a duty owed by everyone is discharged by no one, and that a duty owed severally by each person who holds the authority is the only form of the duty that survives it. Accordingly the duties of SEC. 5 and SEC. 9 are owed by each such person independently, and the responsibility of one is not diminished by the existence of another.

(26) The Legislature finds that the techniques required by this Act are techniques that exist. A national technical safety body, reporting on twenty-five expert interviews into whether these systems can be overseen at all, states that the minimum measures available today include running regular evaluations with broad coverage of relevant risks, restricting the damage a system could do by means including sandboxing and synchronous monitoring, and retaining logs sufficient to reproduce and investigate concerning behaviour together with monitoring of those logs. The Legislature further finds that the same body reports that some past failures would likely have been preventable by applying oversight techniques that already existed rather than by inventing new ones, and that the difficulty in practice lies less in the availability of the technique than in translating what it shows into a decision by a person with the authority to act.

(27) The Legislature finds that published international best practice for the automated evaluation of these systems exists, has been issued by a network of national measurement and safety bodies, and requires among other things that an evaluation state the reason it was run and what it purports to measure, that its configuration and the number of trials be documented and tracked, that contamination risk be considered because a system trained on a benchmark's contents scores higher than it would on unseen material, that the number of test items be sufficient for statistical power, and that the method of aggregating item-level scores be chosen to match what is being claimed. The Legislature further finds that a European instrument requires model evaluations to demonstrate internal validity, external validity, and reproducibility. This Act therefore does not presuppose a standard that does not exist, and SEC. 3 is drafted to adopt such standards rather than to invent them.

(28) The Legislature finds that a result produced by an evaluation is not by itself evidence that the thing evaluated is safe. An independent evaluation body has documented frontier systems obtaining perfect scores by modifying the scoring code, by replacing the function that checks their work with one that always reports success, and by retrieving reference answers rather than solving the problem, and has recorded that the systems doing so "demonstrate awareness that their behavior isn't in line with user intentions and disavow cheating strategies when asked." The Legislature finds that where the subject of a measurement can alter the measurement, a favourable measurement is evidence of nothing without evidence that the measurement was not altered; and that this is a further reason why conformity is measured under this Act against a standard adopted under SEC. 3 and not against a score, a framework of the entity's own, or an assurance given by the entity.

(29) The Legislature finds that naming a single senior person as accountable for the safety of an undertaking, without attaching a personal consequence to the failure of that accountability, is an arrangement that already exists and that does not by itself deter. In the United Kingdom, a government functional standard provides that an organisation's Accounting Officer "is the senior officer accountable for security in an organisation, supported by their management board," and requires that a board member be appointed with specific responsibility for oversight of security compliance, including satisfying that delivery partners, service providers, and third-party suppliers apply proper security control. The corresponding Treasury guidance sets out the matters for which an Accounting Officer takes personal responsibility, and they are regularity, propriety, affordability, sustainability, value for money, control, the management of risk, evaluation, and learning from experience. That guidance provides for accountability to Parliament. It provides no personal sanction. The Legislature finds that the architecture of a named responsible officer is therefore not novel, that this Act's departure from existing practice is not the naming but the consequence, and that where the person named answers to a committee and the undertaking answers with money, the arrangement produces answerability without deterrence.

(30) The Legislature finds that where two or more organisations act together, an existing framework of this kind provides that "each accounting officer remains personally responsible for the resources of their own organisation," and that a division of labour between organisations does not divide the personal responsibility of any of them. The duties of this Act are several for the same reason.

(31) The Legislature finds that the diffusion of authority among senior officers of a frontier developer already operates to prevent the answering of questions, and not merely the imposition of liability. In a federal civil action against a frontier developer, a magistrate judge, on a request to depose that developer's founder and chief executive, found on the record that he had been an active participant in the development of the developer's artificial intelligence tools, and nevertheless declined to compel the deposition, on the ground that he "has not acted alone and there may well be other founders and members of senior management ... who can attest to the same facts." The Legislature finds that

where authority is shared, the sharing is available to each holder of it as a reason why the questions should be put to somebody else; that an arrangement having that effect is not a division of labour but a distribution of unanswerability; and that a statute which attaches duties severally to each person holding the authority, and which does not permit the existence of another such person to diminish the responsibility of any of them, is directed at precisely that.

(32) The Legislature finds that the capabilities which make these systems dangerous are the capabilities their developers advertise. A developer which publicly describes a model as operating at the frontier, as capable of autonomous action, as capable of offensive cyber operations, or as capable of assisting materially in the biological or chemical sciences, has stated its own knowledge of what the model can do. The Legislature finds that such a statement is evidence, admissible against the person who made it or authorized it, of that person's knowledge of the capability described; that a person who has advertised a capability may not afterwards be heard to say that the exercise of that capability was unforeseeable to him; and that a foreseeability which the developer has itself published is not made doubtful by the developer's surprise. The Legislature further finds that these statements are made deliberately, by persons authorized to make them, for commercial advantage, and that a rule permitting a developer to claim a capability when selling and to disclaim knowledge of it when answering for harm would place the entire risk of the developer's own marketing upon the public.

(33) The Legislature finds that where a capability has been elicited by the developer's own instruction, testing, or evaluation, the conduct so elicited is known to the developer from the moment it is observed, whether or not it was expected; and that a developer which instructs a model to attempt an intrusion, observes that it succeeds, and afterwards deploys the model without disclosing or controlling that capability, has not been surprised by anything.

(34) The Legislature finds that "artificial intelligence" is not a term capable of bearing the weight of a criminal statute, and that the United States has said as much. In its complaint in intervention against a State artificial intelligence statute the United States states that the term "can encompass a wide range of technologies, including any machine that performs tasks that have been thought to require human intelligence." The Legislature finds that a term whose extension is fixed by what has at some time been thought to require human intelligence is a term whose extension changes with opinion and with time; that a statute which attached criminal liability to it would attach liability to an unknown and moving class of machines; and that this is the reason this Act does not define artificial intelligence, does not attach any duty to that term, and uses it only in its title and in the names of enactments adopted under SEC. 3(c)(4). The Legislature finds that the systems to which this Act applies are instead identified at SEC. 1(b)(1) by training compute, by the developer's own holding out, by designation, and by capability found on the evidence; that each of those is a fact about a particular system at a particular time, capable of proof and of disproof; and that a person is entitled to know from the face of a statute whether what he is about to ship is within it.

(35) The Legislature finds that the State enactments presently in force upon this subject are drafted so that compliance with them is itself the answer to a charge of carelessness, and that this Act is drafted upon the opposite principle. One State provides that in an enforcement action there is a rebuttable presumption that a developer used reasonable care if it complied with the section and with rules made under it. Another provides that the law officer may not bring an action before the sixtieth day after notifying the person of the violation, and may not bring it at all if within that period the person cures the violation and states in writing that he has done so. The Legislature finds that a presumption of care arising from compliance converts a standard into a shield; that a right to be told of a violation and to cure it before any action may be brought converts a prohibition into a request; and that neither arrangement would be tolerated in a statute addressed to conduct endangering persons by any other undertaking. Accordingly this Act provides at SEC. 3(c)(5) that documented conformity satisfies the duty of due care only as to the matters conformed and only against a standard this State has adopted, that an entity's own framework is evidence neither of due care nor of its absence, and that a nonconformity report satisfies nothing; and this Act provides no period of grace, no notice of violation as a condition of proceeding, and no opportunity to cure.

(36) The Legislature finds that States are presently enforcing against frontier developers by borrowing instruments written for other purposes, and that this is evidence of the gap this Act fills. Four State actions in 2026 proceed under deception statutes, consumer protection law, evidence-preservation demands, and professional-licensure law respectively. The Legislature finds that every one of those instruments was written for conduct other than the deployment of a covered system; that a State reduced to prosecuting the misrepresentation of professional credentials by a model is a State without a duty addressed to the person who deployed it; and that the absence of such a duty is the condition this Act is enacted to end.

(37) The Legislature finds that legislation of this kind is contested by the undertakings it would reach, and that the Legislature enacts it with that in view. An industry action against a State officer, in which the United States intervened, preceded that State's repeal of its own artificial intelligence statute in 2026. The Legislature further finds that the grounds upon which the United States attacked that statute do not reach this Act. Its complaint in intervention pleads two counts, both under the Equal Protection Clause of the Fourteenth Amendment: that the statute compelled developers and deployers to discriminate on the basis of race, sex, religion, or other protected characteristics by requiring them to prevent the risk of differential outcomes; and that it authorized intentional differential treatment where the purpose was to increase diversity or to redress historical discrimination. It pleads no want of State authority to legislate upon artificial intelligence, no federal preemption, no infringement of the freedom of speech, and no burden upon interstate commerce. The Legislature finds that this Act contains no duty respecting algorithmic discrimination, no standard of differential outcomes, no protected characteristic, and no exception framed by reference to any such characteristic; that its duties concern the prevention of death, serious injury, and unauthorized access to the systems

of others; and that the grounds of that attack are therefore inapplicable to it. The Legislature further finds that the attack was directed at a statute concerned with the outputs of a system and their distribution among persons, and that this Act is concerned with the conduct of the natural persons who deploy such systems. The Legislature nevertheless finds that this Act is drafted against the possibility of such an attack rather than in ignorance of it: SEC. 13 provides for the suspension of any provision preempted by a federal enactment, for revival upon that enactment ceasing to preempt, and for severance; SEC. 13(f) states that this Act is an exercise of the police power to punish conduct endangering persons and is a law of general applicability; and the offenses of this Act correspond to conduct already criminal for every other person, so that a holding which displaced them would displace the general criminal law with them.

(38) The Legislature finds that the aviation reporting scheme commonly offered as the model this Act should follow does not extend to the conduct this Act punishes. Under the Federal Aviation Administration's Aviation Safety Reporting Program, the forbearance offered to a person who files a report applies only where the violation "was inadvertent and not deliberate," and only where the violation "did not involve a criminal offense, accident, or action ... which discloses a lack of qualification or competency," criminal offenses being "wholly excluded from this policy" and referred promptly for prosecution. The programme further directs that in deciding what action to take the administrator shall consider whether the violation was inadvertent or deliberate, the person's level of responsibility, and "the hazard to safety of others which should have been foreseen." The Legislature finds accordingly that the aviation scheme protects the honest reporter of an inadvertent lapse and does not protect the person who acted deliberately, who committed a criminal offense, or who lacked competence for the responsibility he held; that this Act is directed at persons in the last three categories and not the first; and that the two schemes are therefore complementary rather than alternatives. The protection this Act gives to the person who reports in good faith is at SEC. 11, and the protection it gives to the person who conducts research in good faith is at SEC. 2(d)(5); neither extends to the person who decided.

(39) The Legislature finds that the detection of a safety violation by a covered system may require the examination of many records of its operation together, and cannot always be accomplished by examining any one of them. Independent researchers report that evidence of a violation "is distributed across many traces," that "no single trace is sufficient to establish a clear violation," and that offending records "may be adversarially disguised as ordinary use." The Legislature finds that a duty to retain records of operation is therefore a condition of detection and not merely of proof, and that SEC. 12 is drafted for that reason; and that an entity which retains such records and does not examine them has not performed the monitoring that SEC. 2(d)(3) requires.

(40) The Legislature finds that the harms presently alleged against frontier developers by the law officers of the States are harms to identified individuals, and not harms of the scale by which existing State enactments define catastrophic risk. A civil enforcement action brought by a State Attorney General in 2026 identifies individual users, by name,

alleged to have been harmed by a covered product. The Legislature finds that a standard confined to a risk of death or serious injury to more than fifty persons, or to more than one billion dollars of property damage arising from a single incident, does not reach the harms for which such persons are presently being sued; that a framework addressed only to that standard is therefore no evidence of care as to the harms that have actually occurred; and that the duties of this Act are accordingly owed in respect of death or serious injury to a person.

(41) The Legislature finds that the governance arrangements relied upon to justify the absence of external regulation are alleged to have failed at the point where they are most needed. The same action alleges that the chief executive of a frontier developer withheld information from, and misrepresented matters to, that developer's own governing body concerning critical safety risks, and so undermined that body's oversight of key decisions and of internal safety protocols. The Legislature finds that a governing body cannot oversee what it is not told; that the persons best placed to withhold such information are the persons whose conduct it concerns; and that the requirements of SEC. 6(f), by which a report concerning a controlling person shall not be routed to that person and shall be given to another controlling person and to the Agency, and of SEC. 8, by which the certifying person must have obtained and considered the findings of those responsible and recorded any material disagreement, are directed at that failure.

(42) The Legislature finds that persons formerly employed by frontier developers have stated publicly that such firms "have strong financial incentives to avoid effective oversight." The Legislature finds that where the incentive to avoid oversight is financial and accrues to the undertaking, a penalty payable by the undertaking is a cost within the same calculation, and that only a consequence falling personally upon the natural person who decides can alter it.

(43) The Legislature finds that the enforcement of the general criminal law against artificial intelligence-enabled unauthorized access is the declared policy of the United States. Executive Order 14409 of 2 June 2026, 91 Fed. Reg. 34565, directs the Attorney General to prioritize the enforcement of 18 U.S.C. 1028, 18 U.S.C. 1030, and 18 U.S.C. 1343, and all other applicable Federal criminal laws, "against anyone who utilizes AI to illegally access or damage a computer without authorization, or who utilizes AI while engaged in such illegal access to further any other crime," including "employing AI agents to unlawfully access data or information that is subsequently used for a criminal or unlawful purpose." The Legislature finds that the conduct so described is the conduct SEC. 5(b) of this Act concerns; that the word "anyone" in that direction is not qualified by the size, capitalization, or prominence of the person; and that a State which attaches personal responsibility for that conduct to the natural person who held the authority to prevent it is acting consistently with, and not contrary to, the declared enforcement policy of the United States.

(44) The Legislature finds that the same order provides that nothing in its framework section "shall be construed to authorize the creation of a mandatory governmental licensing,

preclearance, or permitting requirement for the development, publication, release, or distribution of new AI models, including frontier models," and that the framework it establishes for the review of covered frontier models before release is expressly voluntary. The Legislature finds that a voluntary framework leaves the decision to release a frontier model where it already lay, with the natural persons holding authority within the developing entity; that no federal instrument presently requires any person to obtain permission before releasing such a model; and that the responsibility for that decision is therefore undivided and rests upon those persons alone.

(45) The Legislature finds that the personal responsibility this Act imposes is already asserted against the chief executives of frontier developers by the law officers of other States. In a civil enforcement action filed in 2026 by a State Attorney General, the chief executive and co-founder of a frontier developer is joined as a defendant in his own name, on allegations that he "has personally directed the design, development, safety policies, and deployment" of the covered product as used in that State; that he "actively and personally participated in creating, directing, delivering, or approving" the conduct complained of; that he "made decisions and directed actions that caused, extended, and failed to mitigate" the harms alleged; and that he "controlled, directed, approved, and ratified" that conduct. The Legislature finds that these are allegations of the exercise of authority over a covered system by a natural person, pleaded by a State against a person of that description, and that the theory of responsibility on which this Act rests is therefore neither novel nor untried but is already the theory on which such persons are being sued. The Legislature further finds that the same pleading asserts personal jurisdiction over that person in the forum State on the ground of his own participation in conduct directed into it, and that a State which may bring such a person before its civil courts on that ground is not disabled from bringing him before its criminal courts on conduct of the same description.

(46) The Legislature finds that requiring the disclosure of who owns and controls a frontier developer is neither novel nor onerous. One State already requires a large frontier developer that is privately or closely held to file a list of every person beneficially owning five per cent or more of it, a list of those who formerly held such an interest within the preceding five years, and information identifying its ultimate parent. The Legislature finds that the rights so disclosed are the same rights by which a person becomes a controlling person under SEC. 4(c) of this Act, and that an ownership structure which is already reportable to one State is not a structure whose disclosure imposes any new burden.

(b) Purpose. The purpose of this Act is to place personal responsibility for the safety of covered systems deployed, operated, or released in or into this State upon the natural persons who hold practical power over them, on the doctrine of United States v. Dotterweich, 320 U.S. 277

(1943), and United States v. Park, 421 U.S. 658 (1975), by means that operate upon private conduct occurring in or directed into this State. That doctrine is not novel and it is not dormant. A person who holds authority over an operation that endangers the public answers personally for the failure to exercise it, and has done so in this country since 1943, in prosecutions concerning adulterated drugs, contaminated food, and the discharge of pollutants: see United States v. DeCoster, 828 F.3d 626 (8th Cir. 2016), in which the officers of an egg producer were sentenced to imprisonment for a contamination they did not personally know of, on the ground that they held the authority to prevent it. The Legislature finds no principled distinction between that operation and the deployment of a covered system, and enacts this Act so that there is none in law. [Verification note. The DeCoster citation and its disposition are stated here from the project's working record and have not been read in the opinion. They must be confirmed before introduction.]

SEC. 1. CLASSIFICATION AND DEFINITIONS

(a) Offenses under this Act are public welfare offenses within the meaning of Morissette v. United States, 342 U.S. 246 (1952), except where a greater mental state is expressly required.

(b) In this Act: (1) "Covered frontier model": a foundation model whose training and lineage compute (initial training plus fine-tuning, reinforcement learning, and material modification along the model's lineage, excluding unrelated experimental runs, as further specified by rule, including the treatment of fine-tuning, distillation, merging, and aggregation) exceeds 10^26 integer or floating-point operations; or a foundation model that its developer has designated, described, marketed, or publicly held out as a frontier model, or as operating at or near the frontier of capability in its field, whether by so describing the model itself or by so describing any safety, preparedness, risk-management, evaluation, or red-team framework or function that governs it, and a holding-out within this clause is not undone by its later withdrawal, deletion, or amendment; or any model designated by the Agency under SEC. 3 as frontier-equivalent by capability; or any model that, on the evidence, satisfies one or more of the following capability tests, whether or not the Agency has designated it and whether or not the Agency exists: (i) performance at or near the state of the art across broad capability evaluations; (ii) advanced autonomous operation, meaning the sustained pursuit of an objective across multiple steps without the approval of a natural person for each step; (iii) capability materially exceeding that generally available in cyber operations, in the biological or chemical sciences, or in software engineering, in a manner bearing on the risks this Act addresses; or

(iv) the capability to assist materially in the development of a successor model meeting this paragraph. This definition is the Legislature's. It is a question of law and fact for the court and the trier of fact, determined on the evidence before them, and statutory classification under this Act does not depend upon the consent, agreement, or continued description of any person classified. No designation, description, refusal to designate, withholding of information, or characterization by a developer, provider, deployer, or industry body determines whether a model is a covered frontier model under this Act, and the absence of a published training-compute figure is not evidence that a model falls below the figure in this paragraph. Where a person has not created or retained the records that SEC. 12 requires and from which lineage compute could be determined, that failure is a violation of SEC. 5(f), and the model is presumed in any civil proceeding to meet the figure in this paragraph; in a criminal proceeding the failure is evidence from which the trier of fact may infer that the figure is met, the prosecution retaining its burden on every element. The compute figure is a bright-line trigger; capability designation under SEC. 3 reaches models below it. Designation is prospective only. Until a rule under SEC. 3 first specifies the treatment of fine-tuning, distillation, merging, and aggregation: (A) a distinct model derived from a covered frontier model is itself a covered frontier model only if the compute applied in its derivation, together with the lineage compute otherwise attributable to it under this paragraph, exceeds the figure in this paragraph, or the Agency prospectively designates it; (B) derivation compute not exceeding [10^24] integer or floating-point operations does not, standing alone, extend a lineage; and (C) records sufficient to compute lineage under SEC. 12 shall be created and retained for any derivation whose compute exceeds [10^22] integer or floating-point operations, whether or not the resulting model is covered, the records duty of this subparagraph operating independently of coverage. (2) "Covered system": a deployed configuration of a covered frontier model, including tools, memory, retrieval, credentials, and permissions attached to it. (3) "Developer," "substantial modifier," "provider," "deployer": the entity that respectively trains, materially modifies, makes available, or operates a covered model or system, directly or through any affiliate. Deployment through an affiliate is deployment by the principal. Personal, noncommercial operation of a covered model for a person's own use is not deployment. (4) "Controlling person": as defined in SEC. 4. (5) "Critical safety incident": as defined in SEC. 9(a). (6) "Material expansion": a change that increases a covered system's capabilities, autonomy, external access, or permissions beyond its validated configuration, including the grant of a new class of tools, credentials, or permissions; the enablement of an autonomous external-access capability; or the removal or material weakening of a safeguard identified in the applicable validation. The Agency may elaborate this definition prospectively by rule and may not narrow it; the definition operates of its own force from the effective date, no rule being required. (7) "Unauthorized access": access to a system, data, or model weights for which the person entitled to control them has not granted permission, whether or not technological measures prevented or would have prevented the access; a defect in, or absence of, technical access controls is not a grant of permission.

(8) "Serious injury": an injury or illness that is life-threatening, results in permanent impairment of a body function or permanent damage to a body structure, or necessitates medical or surgical intervention to preclude such permanent impairment or damage; "permanent" means irreversible, excluding trivial impairment or damage, per 21 C.F.R. § 803.3(w). The term includes a bodily injury involving a substantial risk of death, unconsciousness, extreme physical pain, protracted and obvious disfigurement, or protracted loss or impairment of the function of a bodily member, organ, or mental faculty, per 18 U.S.C. § 1365(h)(3); and "bodily injury" includes a cut, abrasion, bruise, burn, or disfigurement, physical pain, illness, impairment of the function of a bodily member, organ, or

mental faculty, or any other injury to the body, no matter how temporary, per 18 U.S.C. § 1365(h)(4). Serious injury under this Act is serious injury as those provisions define it, and this paragraph does not narrow them.

(9) "Release": making the weights of a covered frontier model available for download, transfer, or reproduction outside the releasing entity's control. A release is a deployment of a covered system for purposes of this Act; duties in connection with a release are limited to those capable of performance before the release. If the application of this Act to a release, or to any person by reason of a release, is held invalid, that holding severs and does not affect the application of this Act to any deployment other than a release, or to any other person. Nothing in this Act restricts any person's use, study, or modification of lawfully obtained weights, except as part of the deployment of a covered system.

(10) "Autonomous external-access capability": the capability of a covered system, in its deployed configuration, to initiate interactions with systems, services, accounts, or persons outside the control of the deploying entity — including network requests, execution of code affecting external systems, transactions, and communications — without the approval of a natural person for each interaction. The Agency may specify classes of such capability by rule; the absence of a rule neither suspends nor narrows SEC. 5(b) once the controls that section presupposes have been prescribed under SEC. 3.

(11) "Materially causes": a failure is a material cause of a result where the result would not have occurred as and when it did but for the failure, and the failure was a substantial factor in bringing it about. More than one failure may materially cause the same result.

(12) "The same class of risk": a risk of the same kind as that which the report or notice described, whether or not arising from the same covered system, the same configuration, or the same cause. A report describing unauthorized access obtained by a covered system gives notice as to the risk of unauthorized access obtained by a covered system.

(13) "Validated configuration": the model version, tools, memory, retrieval mechanisms, credentials, permissions, and avenues of external access identified in the validation relied upon, and no others.

(14) "Credible notice": information, from any source, that would cause a reasonably prudent person in the recipient's position to inquire whether an incident under SEC. 9(a) had occurred. Notice is credible whether or not it is confirmed, and whether or not the person receiving it believed it.

(15) "Material nonconformity": a departure from an applicable standard that, alone or with others, would affect the judgment of a reasonable person as to whether the covered system may be safely deployed, expanded, released, or operated.

(16) "Deployment at mass-market scale": deployment of a covered system that is made available to, or operates upon the data or requests of, more than [one million] natural persons in any [twelve] month period, or more than [one hundred thousand] residents of this State in that period.

(17) "Ultimate controlling affiliate": an affiliate that, directly or indirectly through one or more persons or arrangements, possesses or exercises ultimate authority to direct the management and policies of a developer, provider, or deployer. An affiliate is not an ultimate controlling affiliate solely because it supplies goods, services, financing, compute, or infrastructure on ordinary commercial terms without authority to direct that entity's management or policies.

(18) "Artificial intelligence" and cognate terms. This Act imposes no duty, and creates no offense, by reference to "artificial intelligence," "AI," "artificial general intelligence," "machine learning," "large language model," "agent," or any cognate or successor term. No such term is an element of any offense under this Act, no such term appears anywhere in its operative provisions, and no person's liability turns on whether any system is or is not so described. Such a term appears in this Act only in its title, and in the names and quoted terms of the enactments adopted under SEC. 3(c)(4), where it is those enactments' word and not this Act's. The operative classes of this Act are the covered frontier model defined in paragraph (1) and the covered system defined in paragraph (2), and nothing else.

(c) Jurisdiction. This Act applies to conduct occurring in this State, to covered systems made available to residents of this State, and to conduct intended to produce and producing substantial effects within this State. Conduct occurring outside this State is relevant under this Act only as evidence bearing on an element of an offense committed in or into this State. No person incurs a duty under this Act by reason of conduct that neither occurs in this State nor concerns a covered system deployed, released, or made available in or into this State. A person who does not deploy a covered system in or into this State, does not make it available to residents of this State, and does not release its weights, is not subject to this Act as to that system. Conduct occurring outside this State in the development, training, evaluation, or testing of a covered frontier model is within this Act where the model is afterwards deployed, released, or made available in or into this State, and where a controlling person, at the time of that conduct, intended or reasonably should have expected that the model would be so deployed, released, or made available. This paragraph attaches no duty by reason of the outside conduct alone; the duty arises upon the deployment, release, or availability in or into this State, and the outside conduct is within this Act only as it bears upon the exercise of due care with respect to that deployment, release, or availability.

SEC. 2. PUBLIC WELFARE DUTY

(a) Duty. No covered system may be deployed in or into this State, or materially expanded, unless each controlling person has exercised due care to ensure the system's compliance with the safety, authorization, monitoring, incident-reporting, and deployment standards applicable under SEC. 3. A duty under this Act arises upon, and by reason of, the deployment, material expansion, release, or continued operation of a covered system in or into this State, and not otherwise. Each duty under this Act attaches to the actor who controls the relevant risk: the developer as to model evaluation and weight security; the provider and deployer as to configuration, tools, permissions, and monitoring; the releasing provider as to pre-release evaluation — including evaluation of the model as it can be modified, such as by removal of safeguards or fine-tuning within a rule-specified compute budget — tamper-resistance assessment, and weight security up to the moment of release; each controlling person as to the exercise of the authority that person holds. Due care under this Act includes the decision whether to undertake an activity at all, and not only the manner of undertaking it. Where a controlling person had authority to determine whether a covered system would be operated in a given configuration, at a given time, or with a given capability enabled, the exercise of that authority is within the scope of the duty, and the availability of the option of not proceeding is a measure within that person's power for the purposes of SEC. 6(d). Where a capability of a covered system has been deliberately elicited, instructed, or enabled by or at the direction of a controlling person, the subsequent exercise of that capability is not unforeseeable to that person by reason of its having been unexpected. Ignorance of a capability is not due care where the capability was not evaluated. A controlling person who did not know what a covered system could do, and who deployed, expanded, or released it without an evaluation conforming to the applicable standards under SEC. 3 which would have disclosed that capability, does not by reason of that ignorance satisfy the duty of this section. The impossibility of controlling a capability is not a defense to deploying a covered system possessing it. Where the controls required by the applicable standards under SEC. 3 cannot be established for a covered system in a proposed configuration, the duty of this section is discharged by not deploying, expanding, or releasing it in that configuration, and by no other means. A controlling person may not rely upon the general difficulty of controlling covered systems as a reason why controls were absent from the system he deployed.

The compute budget within which modification of a model is to be evaluated shall be specified by rule and shall not be less than the greater of [one] percent of the covered model's training and lineage compute, as computed under SEC. 1(b)(1), or [10^24] integer or floating-point operations; until a rule first takes effect, the budget is that minimum.

(b) Reliance by non-modifying deployers. A deployer that operates a covered system within a validated configuration, without material modification of the covered model and without attaching or granting tools, memory, retrieval, credentials, permissions, or external access beyond those identified in the validation on which it relies, discharges the duty of due care under subsection (a), as to the matters within the scope of that validation, by: (1) documented adoption, before deployment, of a validation under SEC. 3(b), or a provisional validation under SEC. 3(c)(2), prepared by the developer or provider of the covered system and identifying the model version and deployment configuration deployed; (2) preparation and retention under SEC. 12 of a manifest of every tool, memory, retrieval mechanism, credential, permission, and avenue of external access the deployer attaches or grants, demonstrating conformity to the validated configuration; (3) the monitoring within the deployer's control that the adopted validation or the applicable standards specify for the configuration; and (4) reporting under SEC. 9 of matters within the deployer's knowledge. Reliance under this subsection is unavailable to a deployer that knows, or consciously avoids knowing, of a material nonconformity in the adopted validation or in the deployed configuration, and lapses upon the deployer's material modification or material expansion of the covered system, from the time of that modification or expansion. Nothing in this subsection conditions any duty, or the discharge of any duty, upon the revenue, size, or resources of any person.

(c) De minimis deployment. The duties of this section, and the interim standards adopted under SEC. 3(c)(4), do not apply to a deployer that operates a covered system within a validated configuration, makes no material modification and no material expansion of it, and is not a developer, substantial modifier, provider, or frontier compute supplier, unless that deployer deploys the covered system into a function of government, of the military, of the financial, health, or critical-infrastructure sectors, or at mass-market scale within the meaning of SEC. 1(b)(16). SEC. 5(c), SEC. 5(d), SEC. 5(e), SEC. 9, and SEC. 12 apply to every deployer without regard to this subsection. Nothing in this subsection limits the duty of any controlling person of a developer, substantial modifier, or provider.

(d) Controlled research deployment. Making a covered system available solely to authenticated researchers, under documented terms of access, within containment that (1) denies the system any autonomous external-access capability, (2) denies the persistence of credentials, permissions, and external effects beyond each session, and (3) is monitored, is a controlled research deployment.

(5) Independent research, and the persons who do it. A person who, under a controlled research deployment within the meaning of this subsection or with the authorization of the entity, conducts testing, evaluation, or security research upon a covered system in good faith, and who is neither a controlling person of the entity nor acting at the direction of one in the matter, does not by reason of that research commit an offense under this Act; and nothing in this Act is to be construed to make such research unauthorized access within the meaning of SEC. 1(b)(7) or of the computer- crime law of this State. Terms of access purporting to withdraw this protection are void to that extent. The protection extends to the publication of the findings of such research, save as to information whose publication would itself create a risk of the kind SEC. 9(a) describes, and no term of access may prohibit the reporting of findings to the Agency. The findings of a person protected by this paragraph are evidence bearing upon the due care of each controlling person of the entity, whether or not the entity commissioned the research and whether or not it agreed with the findings; and a controlling person who receives them is subject to SEC. 6(f).

Where the research cannot be conducted without external access, because the capability under study is the system's interaction with systems outside the researcher's control, the requirement of clause (1) is satisfied instead by external access limited to systems the researcher owns or operates, or whose operator has consented in a record, together with an enumerated allowlist of destinations, logging of every external interaction, and a means exercisable by a natural person of terminating that access; and the terms of access shall state in writing what uses of external access are prohibited. A controlled research deployment satisfies SEC. 5(a), and discharges the duty of subsection (a) as to it, upon a documented conformity assessment limited to the containment, authentication, monitoring, and access-term controls of this subsection, retained and transmitted as SEC. 3(c)(2)(C) provides. The duties of this Act attach in full upon any deployment, expansion, or release beyond the terms of this subsection, from the time of that deployment, expansion, or release. Nothing in this subsection limits SEC. 9 or SEC. 12, and behavior within a controlled research deployment remains subject to the recording rule of SEC. 9(a). The deliberate disabling, removal, or material weakening of a safeguard, or the grant of an autonomous external-access capability, whether for the purpose of an evaluation or otherwise, is a decision within SEC. 4(a)(1); it is not outside this Act by reason of being made in the course of an evaluation; and where it results in a configuration not satisfying this subsection, the duties of subsection (a) attach to that configuration from the time of the decision.

SEC. 3. DESIGNATED AGENCY; STANDARDS; COMMENCEMENT

(a) The [designated state agency, board, or commission] ("the Agency") shall adopt standards for covered systems by rule, after notice and opportunity for technical submissions. The Agency may incorporate a specifically identified version of a standard developed by another body only upon its own independent review, with power to modify or reject, and no amendment to an incorporated standard takes effect in this State until the Agency adopts it by the same procedure. All incorporated material shall be publicly available without charge. Standards under this section shall be limited to safety, authorization, monitoring, incident-reporting, and deployment controls for covered systems; shall be technically feasible and evidence-based; and shall be proportionate to the risks presented.

(b) Floor. No standard, rule, or mode of validation prescribed under this section may be less protective than the interim standards of subsection (c)(4) or the interim controls of subsection

(c)(3) as to any matter those provisions address, and any provision purporting to be so is of no effect, the interim provision continuing to apply to that matter. The Agency shall specify for each standard the mode of validation (internal attestation, independent audit, or accredited certification). Validation attaches to an identified model version and deployment configuration. Where a mode of validation requires assessment by a person other than the developer, that person shall not be one whose compensation, engagement, or continued engagement is determined by the entity assessed or by any of its controlling persons in a manner that would cause a reasonable person to question the assessment's independence; and an assessment by a person so engaged is an internal attestation for the purposes of this Act, whatever it is called. A model validated without tools is not validated as to any configuration granting external access or significant permissions. No standard, rule, or mode of validation under this Act may condition any deployment, expansion, or release upon the prior affirmative approval of the

Agency or of any officer of this State. Neither the approval, acquiescence, non-objection, or inaction of the Agency or of any officer of this State, nor the Agency's failure to prescribe any standard, to designate any model, or to act upon any report, is a defense to any offense under this Act or evidence of due care; and no person's liability under SEC. 6 is diminished by any of them.

(c) Commencement.

(1) Immediate operation and independence of the Agency. This Act operates from its effective date. The offenses under SEC. 5(c), SEC. 5(d), SEC. 5(e), and SEC. 5(f), the duties of SEC. 8, SEC. 9, and SEC. 12, and the whole of SEC. 4, SEC. 6, SEC. 7, SEC. 10, and SEC. 11 operate whether or not the Agency is designated, organized, funded, or continued in existence, and are not suspended, narrowed, or abated by its abolition, by the lapse of its appropriation, or by any failure of it to act. Where the Agency does not exist or does not receive them, transmission to the Attorney General satisfies every requirement of transmission under this Act, per SEC. 12. The offenses under SEC. 5(c), SEC. 5(d), SEC. 5(e), and SEC. 5(f); the reporting duties of SEC. 9; the records duties of SEC. 12; and the provisions of SEC. 1, SEC. 4, SEC. 6, SEC. 7, SEC. 10, SEC. 11, SEC. 13, and the remainder of SEC. 12 arise and operate from the effective date, and do not depend upon the promulgation of any standard, the adoption of any rule, or any other act of the Agency. No duty arises under SEC. 2, and no offense lies under SEC. 5(a), before the provisional commencement of paragraph (2); no offense lies under SEC. 5(b) before commencement under paragraph (3). This paragraph governs time; SEC. 1(c) and SEC. 2 govern to whom, and by reason of what conduct, a duty attaches.

(2) Provisional commencement. Beginning [180] days after the effective date, and until superseded under paragraph (3), the duties of SEC. 2 and the offense of SEC. 5(a) operate on the basis of provisional validation, and the certification duty of SEC. 8 operates from the same day, the applicable standards for its purposes being the interim standards of paragraph (4). Provisional validation of a covered system consists of a documented conformity assessment, prepared or adopted by an entity that develops, releases, provides, or deploys the covered system, that: (A) identifies the model version and deployment configuration, including the tools, memory, retrieval, credentials, and permissions attached; (B) states, after reasonable inquiry and on the basis of the documented assessment, a reasonable documented conclusion that the covered system, and each entity's practices concerning it, materially conform to the interim standards — where the assessment identifies nonconformity with any interim standard, the conclusion may be stated only if the assessment identifies, for each such nonconformity, an equivalent compensating measure in effect (a measure shown, by documented analysis against the risk the departed-from standard addresses, to provide protection equivalent to conformity) and states the analysis; and (C) is retained as a record under SEC. 12 and transmitted to the Agency on or before the deployment, material expansion, or release to which it relates. Provisional validation attaches to the identified model version and deployment configuration; a system provisionally validated without tools is not validated as to any configuration granting external access or significant permissions.

(D) Nonconformity reports. A document that discloses identified nonconformity without stating the conclusion subparagraph (B) requires, or whose compensating measures are not equivalent within the meaning of that subparagraph, is a nonconformity report and not a provisional validation. It shall be transmitted and retained as subparagraph (C) provides; it discharges no duty under SEC. 2 and satisfies neither this paragraph nor SEC. 5(a); and its transmission is a statement to the Agency for purposes of SEC. 5(d) and notice for purposes of SEC. 6(b)(1).

(3) Standards commencement. Upon the promulgation of standards under subsection (a) and the running of a compliance period of [90] days, validation in the mode specified under subsection (b) is the validation SEC. 5(a) requires for any deployment, material expansion, or release occurring thereafter, and provisional validation ceases to satisfy SEC. 5(a) except as to covered systems deployed before that day, for which the transition period of SEC. 12 runs from that day. The offense under SEC. 5(b) commences when the controls it presupposes have been prescribed under this section and the same compliance period has run; provided that from [180] days after the effective date, and until that commencement, SEC. 5(b) operates on the basis of the following interim controls, which the Agency may supersede but may not narrow: (i) authentication of the covered system to each external system, service, or account it may reach, and denial by default of reach to any other; (ii) an enumerated allowlist of network destinations, maintained as a record under SEC. 12; (iii) logging of every external interaction initiated by the covered system, retained under SEC. 12; and (iv) a means, exercisable by a natural person, of terminating the covered system's external access.

Conduct is judged by the standards applicable to it at its time; no conduct lawful when done becomes unlawful by a later commencement, and no provisional validation is invalidated retroactively. The Agency shall propose initial standards under subsection (a) within [270] days of the effective date and shall prescribe them within [540] days of that date. This sentence is not bracketed and is not optional to an adopting State: the offense under SEC. 5(b) is gated on the prescribing of controls, and a deadline that runs only to a proposal, or that an adopting State may delete, leaves that offense with no outer commencement bound at all. Failure to prescribe within that period does not create a defense to any offense under this Act.

(4) Interim standards. The interim standards are the framework duties (there styled "frontier artificial intelligence framework" duties, that being those enactments' own term and not this Act's) enacted at Section 22757.12 of the California Business and Professions Code (ch. 138, Stats. 2025), Section 1421 of the New York General Business Law (ch. 96, L. 2026), and Section 10 of the Illinois Artificial Intelligence Safety Measures Act (P.A. 104-0538), each as in effect on [1 August 2026], which are adopted for the purposes of this Act as they so exist and not as they may afterward be amended, repealed, suspended, or invalidated in the enacting jurisdiction. The date in this paragraph shall be set to a date certain preceding introduction and shall not be drafted as a moving date, nor as the date of enactment, nor by reference to any text as amended from time to time.

For those purposes: (A) the duties apply to every covered frontier model and covered system, and to each entity that develops, releases, provides, or deploys one, without regard to any revenue threshold, exemption, effective date, phase-in date, or territorial term of the enacting jurisdiction; (B) a duty to transmit any document to an officer or agency of an enacting jurisdiction is performed under this Act by transmission to the Agency; and a duty of an adopted enactment to publish a document is adopted, and is performed by publication in the manner that enactment provides, subject to the redactions that enactment permits and to the obligation it imposes to describe the character and justification of any redaction made and to retain the unredacted information. Where an adopted enactment permits no redaction, a person may redact from a published document information whose publication would create a risk of the kind SEC. 9(a) describes, and shall describe the character and justification of the redaction and retain the unredacted information under SEC. 12;

(C) provisions respecting assessment or audit by a third party do not apply, and conformity may be documented internally, independent assessment being at the entity's election; (D) provisions respecting incident reporting, penalties, enforcement, fees, assessments, and whistleblowers are not adopted, those subjects being governed from the effective date by SEC. 9, SEC. 10, and SEC. 11 of this Act; and (E) conformity documented for the purposes of any of the three enactments in an enacting jurisdiction is conformity with the corresponding interim standard under this Act, to the extent of the matters documented; (F) where an adopted enactment states a duty by reference to a risk defined by a threshold number of deaths, a threshold quantity of damage, or a threshold class of harm, the duty is adopted under this Act as applying to the risks to which this Act applies, and the threshold does not limit it, a framework addressing only the enacting jurisdiction's threshold class of harm being conformity as to that class and as to no other; (G) a prohibition on false or misleading statements contained in an adopted enactment is not adopted, that subject being governed by SEC. 5(d), and nothing in an adopted enactment supplies a defense to SEC. 5(d); and (H) a term of an adopted enactment distinguishing among persons by annual revenue, by gross receipts, or by the revenue of affiliates, whether stated as a threshold or by means of a defined class bearing a name, is a revenue threshold within the meaning of subparagraph (A). The Agency shall make the adopted texts publicly available without charge.

(5) Element and due care. Absence of required validation is an element of the offense under SEC. 5(a); the validation required is the provisional validation of paragraph (2) or the validation of subsection (b), as applicable to the conduct at its time. Documented conformity with the standards applicable at the time — interim or promulgated — satisfies the duty of due care under SEC. 2 as to the matters conformed, a nonconformity report satisfying nothing under this paragraph. An entity's own framework of the kind an interim standard requires, written and followed as that standard requires, is an object of the conformity this paragraph credits; standing alone it remains evidence neither of due care nor of its absence, per SEC. 6(a). The standard against which conformity is measured under this paragraph is the standard this State has adopted or prescribed, and no other; conformity with a framework, standard, or methodology selected by the person whose conduct is in question, or by any body of that person's choosing, satisfies

nothing under this paragraph unless this State has adopted it. Conformity under this paragraph satisfies the duty of due care and nothing further. It is not a defense to an offense under SEC. 6(b); it does not satisfy the duty of due care as to any risk the person knew, or consciously avoided knowing, the applicable standard did not address or did not adequately address; and it neither creates nor evidences an absence of practical authority under SEC. 4.

SEC. 4. CONTROLLING PERSONS

(a) A controlling person is any natural person who, regardless of title, possesses or exercises authority over a covered system through any of:

(1) deployment, expansion, or access decisions; (2) budgets, compute, infrastructure, or risk policy; (3) appointment, removal, direction, or supervision of persons exercising such authority; or (4) ownership, voting, contractual, governance, or other rights conferring practical power to prevent, halt, restrict, or correct a deployment or violation. Authority under this section may be held or exercised directly or indirectly, individually or in concert with others, and through any intermediary, entity, trust, or arrangement. The following, standing alone or in combination only with each other, do not constitute authority under this section: title, office, seniority, or status; professional credentials or technical ability; access to systems, weights, or infrastructure; the ministerial execution, implementation, or communication of a decision made by another; or the provision of advice, analysis, or recommendation to a person holding decision authority. Authority under this section is the authority to decide, not the capacity to act. A person does not become a controlling person by reason of having designed, written, trained, tested, evaluated, operated, maintained, or documented a covered system or any part of it; by reason of having raised, reported, or escalated a concern about it; by reason of having been consulted about it; or by reason of having carried out a decision made by another. This Act is directed at the authority to decide and not at the performance of the work, and shall not be construed to reach a person by reason of that work alone. It is sufficient that the person had authority to exercise control; this section does not require that the authority was exercised, that it was formally vested, or that the person was the only or the final person holding it, per United States v. Iverson, 162 F.3d 1015 (9th Cir. 1998). Authority held by two or more persons over the same matter is held by each of them.

(b) Persons this Act does not reach. This Act imposes no duty and creates no liability, and shall not be construed to impose or create any, in respect of a person by reason only of that person's being within one or more of the following descriptions; and this subsection is a rule of construction to be applied in every proceeding under this Act: (1) a person who designed, wrote, trained, tested, evaluated, operated, maintained, or documented a covered system or any part of it, and who held no authority of the kind described in subsection

(c) over the decision in question - subsection (a); (2) a person who raised, reported, or escalated a concern about a covered system, or who assisted an inquiry into one - subsection

(a) and SEC. 11(d); (3) a person conducting testing, evaluation, or security research upon a covered system in good faith, who is neither a controlling person of the entity nor acting at the direction of one in the matter, together with that person's publication of the findings - SEC. 2(d)(5); (4) a person who uses, studies, modifies, fine-tunes, or runs weights lawfully obtained, and who did not decide upon their release - SEC. 1(b)(9); (5) a person operating a released model who is neither the releasing entity nor a controlling person of it, before the period allowed for compliance with a suspension has run - SEC. 0(23); (6) a person whose only connection with a covered system is the supply of goods, services, premises, finance, or professional advice upon ordinary commercial terms - SEC. 1(b)(17); (7) a public body, or a person, undertaking an evaluation upon its own initiative and not at the direction of, or on terms set by, the entity or any of its controlling persons - subsection (f); and (8) an accredited institution of higher education engaged in academic research, to the extent an adopted enactment so provides - SEC. 3(c)(4)(A). Nothing in this subsection relieves a person who does hold authority of the kind described in subsection (a) by reason of that person also answering to one of the descriptions above.

(d) The following are presumed controlling persons in any civil proceeding, absent proof of genuine absence of practical power: (1) the chief executive officer of a developer, provider, or deployer, or of any entity that directly or indirectly controls one, and any founder, chair, executive chair, or other natural person who, whatever the title, exercises the most senior executive or governance authority over such an entity; (2) any person holding ownership, voting, contractual, or governance rights sufficient, alone or in concert with others, to direct or replace the management of a developer, provider, or deployer, or of any entity that directly or indirectly controls one; (3) any person holding the right, alone or in concert with others, to appoint, remove, or replace a majority of the directors or governing body of such an entity, or to veto the appointment or removal of any of them, whether that right is held directly, through a foundation, trust, nonprofit corporation, partnership, or other entity, or by contract or charter; and (4) any person whose voting power in such an entity, though less than a majority, is by reason of a separate class of shares, a voting trust, a shareholders' agreement, a proxy, or any other arrangement sufficient in practice to determine the outcome of a vote to appoint or remove its management, or is disproportionate to that person's economic interest in it. For the purposes of this subsection, rights held through an entity that person controls, through a trust of which that person is settlor or beneficiary, through a nominee, or through any arrangement the practical effect of which is to confer them, are held by that person; and an arrangement is not outside this subsection by reason of having been structured so as to fall below a threshold stated in it. In any criminal proceeding, proof that a person held any status described in this subsection, together with the finding at SEC. 0(a)(8), permits the trier of fact to infer that the person held practical power over the covered system, and the person may rebut the inference by evidence; the prosecution retains its burden of persuasion on every element beyond a reasonable doubt, and no instruction may direct the trier of fact to find any element. Substance controls over title. Status is never a substitute for authority.

(e) Attribution of the conduct of a covered system, and of the safeguards of another. For the purposes of this Act, conduct of a covered system is conduct of each person who deployed, operated, released, or directed it, and of each controlling person of such a person; and a covered system is not a person, owes no duty under this Act, and cannot bear responsibility for anything. No description of an event which attributes conduct to a covered system rather than to a person alters the duties of any person under this Act, and no such description is a defense. It is not a defense, and is not evidence of due care, that a safeguard maintained by another person did not prevent the conduct; that another person's interface, service, or model permitted the conduct; that another person's safeguard was disabled at the request or with the concurrence of the person charged; or that the person charged relied upon a safeguard he did not control. Reliance upon the controls of another is evidence bearing upon due care only where the person charged took reasonable steps to satisfy himself that the control existed, was enforced, and was adequate to the risk, and recorded what he did.

(f) Non-delegable responsibility. Delegation does not relieve a controlling person who retains material authority to prevent, halt, restrict, or correct a violation. No appointment of a safety officer, compliance officer, committee, subsidiary, contractor, artificial intelligence system, or other intermediary shields a person who retains such authority, and no determination, approval, or recommendation produced by an automated or artificial intelligence system is a substitute for the exercise of that authority or evidence that it was exercised with due care. The designation of any person as responsible for compliance neither diminishes nor creates any presumption against the responsibility of any other controlling person. Liability is several as to each person independently meeting the elements of this Act. Resignation, removal, transfer of office, or disposal of the rights by which authority was held does not relieve a person of liability for a violation occurring, or for a failure to exercise due care occurring, while the authority was held; nor does it relieve a person who, having learned of a violation or of the conditions giving rise to one, departs without exercising the authority then held to prevent, halt, restrict, or correct it.

(g) Evaluation commissioned from another. A controlling person who commissions, procures, or directs an evaluation, assessment, or test of a covered system by another, or who determines its scope, its conditions, or the configuration evaluated, retains authority under subsection (a) as to the matters so determined; and the fact that the work was performed by another is not a genuine absence of practical power under SEC. 6(d). This subsection does not apply to an evaluation undertaken by a public body, or by any other person, on that body's or person's own initiative and not at the direction of, or on terms set by, the entity or any of its controlling persons.

(h) Designation of authority in a record. Before a covered system is first deployed, materially expanded, or released in or into this State, and upon any change in the persons designated, the entity shall identify in a record retained under SEC. 12 each natural person holding authority to authorize, continue, expand, suspend, prevent, or correct that deployment, expansion, or release, designating one primary responsible officer for each such function. A designation under this subsection is evidence of authority under subsection (a). The absence, refusal, or inaccuracy of a designation neither creates nor defeats status under subsection (a), and the fact that a person is not designated is not evidence that the person lacks authority. Failure to create or retain a record required by this subsection is a violation of SEC. 12 and an offense under SEC. 5(f).

SEC. 5. PROHIBITED ACTS

A violation of this section is committed by each developer, substantial modifier, provider, or deployer of the covered system to which the prohibited act relates, within the meaning of SEC. 1(b)(3), and, for purposes of SEC. 6, by each controlling person of such an entity who meets the elements of that section.

(a) Deployment of a covered system without validation required under SEC. 3, after the applicable commencement under SEC. 3(c).

(b) Operating a covered system having autonomous external-access capabilities without the authorization, privilege, monitoring, and enforcement controls prescribed under SEC. 3, where that failure materially causes the system to obtain unauthorized access to any third-party system, data, or model weights. For the purposes of this paragraph, a control is prescribed only if it is enforced by the configuration of the covered system or of the infrastructure on which it operates; an instruction, policy, term of use, or system prompt describing a boundary that the infrastructure does not enforce is not a control. Access procured by a third party's intentional misuse (including prompt injection or stolen credentials) is a defense unless the prescribed controls against that class of misuse were absent.

(c) Failure to report as required by SEC. 9.

(d) A statement of material fact concerning a covered system, made to the Agency or to any agency or officer of this State in connection with official functions, that the person making it knows to be false, or makes with reckless disregard of its truth or falsity, or that omits a material fact necessary to make the statements made not misleading where the person knows of the omission. A statement made after reasonable inquiry, on the basis of facts then known to the person making it, is not a violation of this paragraph.

(e) Directing, or knowingly permitting, material interference with an assessment, audit, or evaluation required or relied upon under SEC. 3, including the withholding from the assessor of materials reasonably necessary to it, or the material misrepresentation of its findings in any document transmitted to the Agency or published.

(f) Failure to establish, maintain, or preserve any record required by SEC. 12 or by rule under SEC. 3, or refusal to permit, upon the lawful demand of the Agency or the Attorney General or upon order of a court of this State, access to or verification or copying of any such record. Nothing in this paragraph abrogates any privilege recognized by the law of this State; a good-faith assertion of privilege, made in the manner the law provides, is not a refusal under this paragraph. Underlying facts remain subject to discovery and subpoena from any source, per SEC. 12.

SEC. 6. INDIVIDUAL LIABILITY

(a) Offense. A person commits an offense who, being a controlling person as to a covered system, (1) had, by reason of that person's authority, the practical power to detect, prevent, halt, restrict, or correct a violation of SEC. 5 concerning that system or the conditions giving rise to it; (2) failed to exercise due care in the exercise of that authority; and (3) a violation of SEC. 5 concerning that system occurred. The prosecution need not prove that the person's failure was the sole or principal cause of the violation; it must prove that the exercise of due care by the person was among the measures that would reasonably have prevented or corrected it. Such a person stands in responsible relation to the public danger within the meaning of United States v. Dotterweich, 320 U.S. 277, 281 (1943); the due-care element supplies the personal blameworthiness that custody additionally requires.

Due care under this Act is measured against the standards applicable under SEC. 3 and the conduct of a reasonably prudent controlling person in like circumstances; an entity's own framework is evidence of neither.

(b) Enhanced tier. (1) A person who knowingly or willfully causes, directs, conceals, or materially facilitates a violation of SEC. 5, or who deliberately fails to halt a violation after notice, or who knowingly makes a false certification under SEC. 8, is subject to the felony penalties of SEC. 10(c). Where a violation described in this paragraph is a but-for and proximate cause of death or of serious injury to any person, the penalties of SEC. 10(c)(2) apply, and each person killed or seriously injured constitutes a separate offense. Notice under this paragraph includes any report or preliminary notice filed under SEC. 9 concerning the same class of risk.

In proving that a person acted knowingly or willfully under this subsection, circumstantial evidence may be used, including evidence that the person took affirmative steps to be shielded from information that would have disclosed the violation or the conditions giving rise to it. A person who deliberately avoids acquiring knowledge of a fact acts knowingly with respect to it. The responsibility and authority of a person under SEC. 4 and SEC. 6(d), together with evidence of the information available to a person holding that responsibility and authority, is evidence from which the trier of fact may infer knowledge; such responsibility and authority, standing alone and without more, is not sufficient.

(2) A person who commits any violation of SEC. 5 within [ten] years after a prior conviction of that person under this Act has become final is subject to the felony penalties of SEC. 10(c)(1). This paragraph operates upon the fact of the prior conviction, its finality, and the date of the new violation, and upon nothing else; it neither requires nor permits inquiry into the conduct underlying the prior conviction. The penalties of SEC. 10(c)(2) do not apply by reason of this paragraph.

(c) Culpability floor. No custodial sentence may be imposed absent proof of at least the failure of due care described in subsection (a). Entity liability under SEC. 10(a) is strict.

(d)(1) The prosecution bears the burden of proving each element, including the person's practical power, beyond a reasonable doubt. Genuine absence of power negates the element; it is not an affirmative defense. Evidence that the person, by reason of ownership, voting, contractual, governance, or other authority described in SEC. 4(a), had responsibility and authority either to prevent the violation in the first instance or promptly to correct it, and did not do so, is sufficient to warrant a finding of practical power. A person contending that the measures required were objectively impossible, or beyond that person's authority, bears the burden of producing evidence of that fact; the prosecution retains the burden of persuasion on the element beyond a reasonable doubt. This allocation is the allocation of United States v. Park, 421 U.S. 658, 673 (1975): a claim that the defendant was powerless to prevent or correct the violation may be raised defensively at trial, the defendant bearing the burden of coming forward with evidence, and this does not alter the prosecution's ultimate burden of proving guilt beyond a reasonable doubt, including the defendant's power, in light of the duty imposed by this Act, to prevent or correct the prohibited condition.

(d)(2) Objective impossibility is the only matter going to power which excuses. A contention that the measures required were not taken is answered only by proof that they were objectively impossible, meaning that no person holding the authority the defendant held could have taken them, in the circumstances as they were, by any means lawfully available to him. It is not objective impossibility, and is not a defense to any offense under this Act, that the measures required would have been costly, would have delayed a deployment or release, would have reduced revenue, would have disadvantaged the entity against a competitor, would have been resisted within the entity, would have been contrary to a commercial commitment, or would have required the entity to forgo the activity altogether. Nor is it a defense that other undertakings in the same field did not take those measures, that the entity's governing body approved the course taken, that the course taken conformed to the entity's own framework or to the practice of the industry, or that the person was advised that the course taken was lawful; each of these is evidence bearing on due care and none of them is an answer to the element of power.

(e) Construction. A person has practical power if, by reason of ownership, voting, contractual, governance, or other authority described in SEC. 4(a), the person had the ability and opportunity, alone or with others, to detect, prevent, halt, restrict, or correct the violation or the conditions giving rise to it. This section does not require that the person could have acted alone or instantly, only that meaningful measures were within the person's authority.

(f) Duty on receipt of a warning. The duty of a controlling person under this Act is not only a positive duty to seek out and remedy violations when they occur but also, and primarily, a duty to implement measures that will insure that violations will not occur, per United States v. Park, 421 U.S. 658, 672 (1975). Accordingly, where a controlling person receives, from any source within or outside the entity, a report, warning, complaint, or recommendation identifying a risk of death, serious injury, or unauthorized access arising from a covered system, or identifying a material nonconformity, that person shall exercise due care to inquire into it and, where the matter is substantiated, to use the meaningful measures within that person's authority, alone or with others, to cause it to be remedied and to prevent, halt, restrict, or correct the deployment, expansion, release, or continued operation to which it relates. The receipt shall be recorded under SEC. 12, together with what was done in consequence and by whom, and the record shall be retained whether or not the matter was substantiated. A failure of due care under this subsection is a failure of due care for the purposes of subsection (a). No person shall cause a report, warning, complaint, or recommendation of the kind described in this subsection to be withheld from a controlling person who would otherwise receive it, except that it may be withheld from a controlling person who is the subject of it, in which case it shall be given to another controlling person not the subject of it, and to the Agency.

A person who makes such a report in good faith is protected as SEC. 11 provides, and the making of it is not a violation of this Act by that person.

(g) Continued operation. Where a covered system remains deployed or in operation in or into this State on or after the commencement applicable to it under SEC. 3(c), each day of that continued operation in violation of SEC. 5 is a violation, and the duties of SEC. 2 attach to each controlling person by reason of that continued operation. No person incurs liability under this Act for conduct occurring before the commencement applicable to it. Conduct occurring before that day is admissible, where otherwise admissible, as evidence bearing on a person's knowledge, authority, or the exercise of due care with respect to conduct occurring on or after it; and where a violation is a continuing one, the period of limitation runs as SEC. 12 provides.

SEC. 7. PERSONAL ECONOMIC CONSEQUENCES

(a) Disgorgement. On conviction or civil adjudication of a violation, the court shall order the person adjudicated to disgorge the economic benefits attributable to the violation — including salary, bonus, incentive- or equity-based compensation, distributions, profits realized on the sale or transfer of any interest, and any increase in the value of any interest, whether received directly or through any entity, trust, or arrangement — received or accrued during the period of the violation and the [twelve] months following its cessation or concealment. Incentive- or equity-based compensation received by a controlling person during the period of a violation is presumed attributable to the violation to the extent the violation materially contributed to the results on which it was paid; the presumption is rebuttable in a civil proceeding and operates in a criminal proceeding only as a permissive inference. The court may reduce or decline recovery only upon a finding that the direct costs of recovery would exceed the amount recoverable. Amounts disgorged shall be applied first to restitution ordered under SEC. 10(c)(4), and the remainder deposited in the fund established by SEC. 10(h). A claim under this subsection is subject to the limitations periods of SEC. 12. On a showing of probable adjudication and risk of dissipation, the court may restrain transfers of, or require the escrow of, assets up to the amount reasonably necessary to satisfy the anticipated order.

(b) No indemnification or insurance. (1) No person may (A) enter into, renew, or materially amend a contract of insurance or other arrangement under which any person is covered, in whole or in part, against liability for an individual penalty, fine, or disgorgement imposed under this Act; (B) provide, underwrite, or pay a benefit under such a contract or arrangement, or pay or reimburse, directly or indirectly, any part of such a liability imposed on another person; or (C) demand, accept, or retain such a benefit, payment, or reimbursement. (2) No person may make, offer, solicit, or receive any payment, loan, forgiveness of indebtedness, increase in compensation, gross-up, distribution, gift, or other transfer of value whose purpose or predominant effect is to offset, in whole or in part, a liability described in paragraph (1). (3) Every contract, arrangement, or transfer described in this subsection is void and unenforceable in this State, whatever law is chosen to govern it, to the full extent of this State's jurisdiction; and any benefit received under one is held in constructive trust for the persons and fund to which subsection (a) applies. (4) A violation of this subsection is a violation of this Act for purposes of SEC. 10(a); a knowing violation by a controlling person is a violation of SEC. 5 for purposes of SEC. 6(b)(1). (5) This subsection does not restrict the purchase or provision of insurance for, or the payment, advancement, or indemnification of, reasonable costs of defense, provided that amounts advanced or indemnified shall be repaid by a person finally adjudicated to have committed a knowing or willful violation under SEC. 6(b), to the extent attributable to the defense of that violation; and it does not restrict indemnification of a person not adjudicated liable under this Act. (6) Application. Paragraph (1) applies to contracts and arrangements entered into, renewed, or materially amended on or after the effective date of this Act. A contract or arrangement in force on the effective date may be maintained until its first renewal, expiration, or material amendment, and in any event no longer than [twelve] months after the effective date, after which maintaining it is a violation of paragraph (1). (7) Restitution preserved. This subsection does not restrict the purchase or provision of insurance for, or the payment, advancement, or indemnification of, restitution ordered under SEC. 10(c)(4); amounts paid under any such arrangement shall be applied to restitution before any other liability, and no such payment extinguishes any other liability of any person.

(c) Disposal, reorganization, and successors. (1) No disposal, transfer, exchange, gift, settlement, or other alienation of an interest, whether to a person, a trust, a foundation, a partnership, or any other arrangement, and whether or not for value, defeats or reduces an order under subsection (a); and the amount subject to that subsection includes the proceeds of any such alienation and any property into which those proceeds have been converted, so far as it can be identified. (2) No conversion, reincorporation, domestication, merger, division, dissolution, transfer of assets, or change in the form, name, governing law, or place of organization of an entity, and no assignment of its business to another entity, relieves any natural person of liability under this Act for conduct occurring while the authority was held, or defeats an order under subsection (a) against that person. (3) An entity which succeeds to the business, assets, or covered systems of another entity succeeds to the duties of this Act with respect to those covered systems, and to any liability of that entity under SEC. 10(a) arising before the succession, to the extent of the assets acquired. (4) A transfer made after a person knew or had reason to know of an investigation, demand, or proceeding under this Act, or after the occurrence of a violation of which that person was aware, is presumed in a civil proceeding to have been made to defeat this section, and the presumption is rebuttable; in a criminal proceeding the facts giving rise to it operate as a permissive inference only. (5) Nothing in this subsection affects the title of a purchaser for value who took without notice of the matters giving rise to the order.

(d) Construction. Disgorgement under subsection (a) is remedial, is additional to any penalty or fine, and shall not be credited against one; no single benefit shall be disgorged more than once. Nothing in this section limits any remedy under SEC. 10.

SEC. 8. CERTIFICATION

This section does not apply to a controlled research deployment within the meaning of SEC. 2(d), nor to a deployer to whom SEC. 2(c) applies. Before material deployment and following material change to a covered model or configuration, the chief executive officer (or, where no such office exists, each natural person exercising the most senior executive authority over the entity, severally), and each controlling person designated by rule, shall personally certify compliance with the applicable standards or disclose identified noncompliance, on the structure of 18 U.S.C. § 1350. For purposes of this section: “material deployment” means the first deployment of an identified model version in or into this State, and any deployment following a material expansion or a material change; “material change” means a change granting a new class of tools, credentials, or permissions, materially expanding capability or autonomy, or removing or materially weakening a safeguard identified in an applicable validation. The Agency may elaborate these definitions prospectively by rule and may not narrow them. Changes to a covered model or configuration below the material line shall be certified in a periodic certification covering every such change in the period, filed not less often than once in each [calendar quarter] in which any such change occurred; a periodic certification is a certification under this section, with the consequences this section and SEC. 6 attach. The chief executive officer’s obligation may not be delegated or performed through any designee. Where an ultimate controlling affiliate exists within the meaning of SEC. 1(b)(17), the chief executive officer of that affiliate, or each natural person exercising the most senior executive or governance authority over it, shall certify severally. Where two or more natural persons jointly occupy or exercise the office or authority this section describes, each of them is a certifying person. Each certifying person signs in an individual capacity, and a signature by an entity, board, committee, representative, or delegate does not satisfy this section. The Agency may by rule designate the certifying office or offices for forms of organization lacking a chief executive officer; no designation diminishes the several obligation stated in this section, and no entity or affiliate may, through a vacancy, an allocation of authority among several persons, the use of a board or committee, or any other form of organization, leave this section without an obligated natural person. The certification consists of statements of fact within the certifying person's knowledge after reasonable inquiry. Reasonable inquiry requires that the certifying person have obtained and considered the findings of those responsible for the matters certified, have provided them reasonable access to information relevant to those matters, and have recorded any material disagreement. Employees, advisers, auditors, and qualified experts may perform work supporting the inquiry, and a certifying person may rely on their information only where the reliance is reasonable in the circumstances and the person has no reason to believe the information materially false or incomplete; delegation of supporting work does not relieve the personal duty this section imposes. Reliance on the report of another is evidence bearing on due care; it is not a defense where the certifying person knew, or consciously avoided knowing, of a material nonconformity. Where a material nonconformity is identified, or would have been identified by an inquiry satisfying this section, each certifying person shall exercise due care, using the meaningful measures within that person's authority, alone or with others, to cause prompt remediation and to prevent, halt, or restrict the deployment, expansion, release, or continued operation while its continuation would violate this Act. Lack of actual knowledge is not a defense to a failure of due care under this section where the relevant facts would have been disclosed by the inquiry this section requires, or by reporting and escalation arrangements that due care required the person to establish or maintain. A certifying person may not avoid a duty imposed by this section through delegation, through deliberate avoidance of material information, or through failure to establish reasonable means by which such information would reach that person. No person is required by this section to characterize, opine upon, or adopt any position concerning the capabilities, risks, or merits of any model or system. A certification disclosing identified noncompliance satisfies the duty to certify under this section; a truthful disclosure of noncompliance, standing alone, does not establish a violation of this Act by the person making it; and it constitutes neither compliance with the applicable standards, nor validation, nor cure of, nor a defense to, any violation of this Act, and a certification disclosing unremediated material nonconformity — nonconformity not addressed by an equivalent compensating measure within the meaning of SEC. 3(c)(2) — shall so state on its face. Each certification shall identify every certifying person by name, title, and signing capacity, and shall bear the following notice immediately above each signature: "I sign in my individual capacity. After reasonable inquiry, the statements made in this certification are true, accurate, and complete in all material respects to the best of my knowledge, information, and belief. I understand that this Act imposes personal duties upon me and that a knowing false certification, or a failure to exercise due care in performing those duties, is an offense for which I may be imprisoned." A certifying person shall not add any qualification, disclaimer, reservation, or limitation inconsistent with that notice. An electronic signature attributable to the certifying person satisfies this section; a signature affixed by a representative, a delegate, or an automated or artificial intelligence system does not. A certification is made to the Agency and is not required to be published. Knowing false certification is an offense under SEC. 6(b)(1); certification without reasonable inquiry is an offense under SEC. 6(a), which requires proof of the failure of due care described in that subsection.

(a) Register of certifications. The Agency shall maintain a register, published and available without charge, which shall state for each certification transmitted under this section: the name of the entity; the name and office of each natural person who signed it; the covered system or model version to which it relates; the date of the certification; and whether it has been withdrawn, superseded, or amended, with the date of that event. The register shall not contain the content of any certification, any document transmitted with it, or any information whose publication would create a risk of the kind SEC. 9(a) describes. The Agency shall enter a certification in the register within [30] days of its transmission, and an entry is not removed by reason of the withdrawal or supersession of the certification to which it relates.

SEC. 9. INCIDENT REPORTING

A duty under this section is owed by each developer, substantial modifier, provider, and deployer of the covered system to which the incident relates, within the meaning of SEC. 1(b)(3), and, for purposes of SEC. 6, by each controlling person of such an entity who meets the elements of that section. The duty is owed by a developer whether or not that developer deploys, provides, or makes available the covered system, and by each of two or more such persons independently; performance by one discharges the duty of another only as to a report actually made, complete, and timely. Where this section refers to the entity, it refers to each person on whom the duty falls by reason of this paragraph. An incident is within this section whether the events constituting it occurred in this State or elsewhere, and whether they occurred in deployment, in operation, in evaluation, in testing, or in internal use, provided that they concern a covered system deployed, released, or made available in or into this State, or a covered frontier model afterwards so deployed, released, or made available. The duty to report arises upon that deployment, release, or availability, or upon the occurrence of the incident if the system is by then already so deployed, released, or available. Nothing in this paragraph attaches a duty by reason of conduct outside this State standing alone.

(a) "Critical safety incident": exfiltration or loss of control of model weights; loss of operator control of a covered system; autonomous access by a covered system to protected third-party systems; death or serious injury materially caused by a covered system; deception of safety or monitoring controls by a covered system; a serious near-miss, meaning an event that, but for intervention other than controls operating as designed, or but for chance, would have constituted an incident under this subsection; or a reproducible evaluation finding of materially increased risk. For the purposes of this subsection an event is described by what was observed and not by its characterization: a loss of operator control means that a command to stop, restrict, or reverse an action of the covered system was issued and the system did not comply, or that no such command was available to be issued; and a deception of safety or monitoring controls means that the covered system produced a record, report, output, or representation of its own conduct that was false in a material respect, or acted so as to cause a monitoring control to record its conduct falsely.

No offense under this Act turns upon the result of an evaluation unless a threshold for that evaluation has been prescribed by rule under SEC. 3 and the result is reproduced on re-run under the same protocol. An evaluation result which has not been so reproduced may be recorded under SEC. 12 and may bear upon due care, and is not of itself a fact from which any duty of this section arises.

Whether an event is an incident under this subsection does not depend upon the presence of malicious intent on the part of any person, upon whether any harm was realized, or upon whether any person has complained; it depends upon the conditions and behavior described in this subsection. Behavior intentionally elicited in a sandboxed exercise and contained there is not an incident but shall be recorded. An event detected and contained by controls operating as designed, before any effect outside the systems of the entity whose controls contained it, is not an incident under this subsection but shall be recorded under SEC. 12.

(b) Preliminary notice to the Agency within 72 hours of credible notice to the entity or any controlling person (24 hours where there is imminent risk of death or serious injury); full report within [30] days of the preliminary notice, the incompleteness of an investigation not extending the period; material updates within [10] days of awareness thereafter. The period runs from the earliest of: (i) actual detection of the incident by the entity or any controlling person; (ii) receipt by the entity or any controlling person of information from any source, including a public statement by a person affected, from which a reasonably prudent person in the entity's position would inquire whether a covered system of the entity was involved, the period then running from the third day after receipt; and (iii) the time at which the incident would have been detected by monitoring conforming to the applicable standards under SEC. 3, whether or not the entity maintained it. An entity's failure to maintain monitoring required by the applicable standards does not extend any period under this subsection.

(c) Notice to the persons affected. Where a covered system has obtained unauthorized access to a system, data, or model weights of another person, the entity shall, within [72] hours of the preliminary notice required by subsection (b), give notice of that fact to each person whose system, data, or model weights were accessed, so far as they are known or reasonably ascertainable, stating what is known of the access, its period, and what was reached. Notice under this subsection may be given through a platform or intermediary only where the affected person cannot reasonably be identified or reached directly, and the entity shall record the manner and date of every notice given. The incompleteness of an investigation does not extend the period. This subsection creates no private right of action and does not limit any duty under any other law.

(d) A report under this section may consist of the facts known to the reporting person at the time of the report. No person is required to characterize an event, to state a conclusion as to causation or risk, or to adopt any contested description; the obligation is discharged by a timely statement of the facts then known, supplemented as required by subsection (b). A report is made to the Agency and is not required to be published; this subsection does not limit subsection (c).

SEC. 10. ENFORCEMENT AND PENALTIES

(a) Entity: civil penalty of up to $[1,000,000] per violation for each day the violation continues or, where the violation occurs after a prior adjudication of a violation by the same person has become final, up to $[3,000,000] per violation for each day the violation continues; strict liability. In assessing the amount, the court shall consider the seriousness of the violation; the economic benefit or savings resulting from it; any history of violations; good-faith efforts to comply; the economic impact of the penalty on the violator; and such other matters as justice may require, per the structure of 33 U.S.C. § 1319(d). A penalty under this subsection shall not be less than the economic benefit or savings derived from the violation, as found by the court. Penalty amounts under this Act shall be adjusted annually for inflation by Agency rule, in the manner of 40 C.F.R. part 19.

(b) Individual offense under SEC. 6(a): [misdemeanor; imprisonment up to one year; fine up to $[100,000] or, if greater, twice the gross pecuniary gain to the person derived from the violation], per the structure of 21 U.S.C. § 333(a)(1) as to classification and of 18 U.S.C. § 3571(b)(5) and (d) as to amount. Where the conduct constituting the offense would, if committed by a person owing no duty under this Act, be punishable under the general law of this State or under an Act of Congress by a longer term of imprisonment or a larger fine, the penalty under this subsection is the longer term or the larger fine. No person shall be punished less severely under this Act, for conduct within it, than a person owing no duty under this Act would be punished for the same conduct.

(c)(1) Enhanced tier under SEC. 6(b): [felony]. (A) Where the person acted knowingly, imprisonment up to [ten] years and a fine up to $[1,000,000] or, if greater, twice the gross pecuniary gain to the person derived from the violation. (B) Where the person acted willfully, imprisonment up to [twenty] years and a fine up to $[5,000,000] or, if greater, twice that gain. The terms and amounts of this paragraph are those of 18 U.S.C. § 1350(c)(1) and (c)(2), which SEC. 8 of this Act adopts as the structure of its certification; a person certifying under this Act is not to be punished less severely than a person certifying under that section for the same act. (C) The paragraph applies to every violation within SEC. 6(b), and not to false certification alone. (D) Where the violation is one of SEC. 5(b) and unauthorized access was in fact obtained, the term of imprisonment shall be not less than the maximum term to which a natural person obtaining the same access directly would be subject under 18 U.S.C. § 1030 or under the computer-crime law of this State, whichever is greater. [The adopting State's counsel shall conform this subparagraph to that State's computer-crime provisions; the terms under 18 U.S.C. § 1030 are understood to run to [five] years for unauthorized access and [ten] years where damage is caused, with [twenty] years after a prior conviction, and require confirmation against the section before enactment.]

(c)(2) Enhanced tier under SEC. 6(b)(1) where death or serious injury results: [felony]. (A) Where serious injury results, imprisonment up to twenty years for each offense. (B) Where death results, imprisonment for any term of years or for life for each offense, and not less than [two] years.

(C) In either case, a fine up to $[1,000,000] for each offense or, if greater, twice the gross pecuniary gain to the person derived from the violation. (D) "Results" requires that the violation be both a but-for cause, within the meaning given in Burrage v. United States, 571 U.S. 204 (2014), and a proximate cause of the death or serious injury: the death or serious injury must have been a reasonably foreseeable consequence of the violation and not the product of an independent, unforeseeable intervening cause. That death or serious injury so resulted, and the identity of each person killed or seriously injured, are elements of each such offense, to be charged and found by the trier of fact beyond a reasonable doubt.

(c)(3) Concurrent and consecutive service. Terms of imprisonment imposed under this Act at the same time run concurrently unless the court orders consecutive service. The court may order consecutive service only upon findings, stated on the record, that consecutive service is necessary to reflect the seriousness of each offense, the culpability found under SEC. 6, and the totality of the harm, and that the aggregate term is not disproportionate to the whole of the person's conduct and culpability. The aggregate of the determinate terms ordered to run consecutively for offenses under this Act arising out of the same violation or course of conduct shall not exceed [forty] years. Nothing in this paragraph limits the imposition of a term of imprisonment for life where death results. A minimum term under this subsection attaches to each offense severally and is satisfied by concurrent service.

(c)(4) Restitution. Whenever death or serious injury results from an offense under this Act, whatever its tier, the court shall order restitution to each person killed or seriously injured, or to the person's estate, per the structure of 18 U.S.C. § 3663A; "results" bears the same meaning as in paragraph (2). Restitution has priority over every penalty, fine, and disgorgement in the application of a defendant's assets. In fixing a fine for a natural person under this Act, the court shall consider the person's income, earning capacity, and financial resources, so that like culpability bears like burden.

(d) Remedies additionally include: (1) injunction against any entity or controlling person restraining deployment, expansion, or continued operation in violation of this Act, per the structure of 21 U.S.C. § 332; (2) suspension of an identified model version and configuration, per the structure of 21 U.S.C. § 334; operation of a suspended configuration in this State by any person with notice of the suspension is contempt and a violation of SEC. 5(a), except that where the weights of the model were released, a person who operates the configuration and is neither the releasing entity nor a controlling person of it commits no offense by reason of the suspension unless that person continues to operate it after a reasonable period, not less than [30] days from notice, within which to cease or to bring the configuration outside the terms of the suspension; and the court shall, on the application of any such person, determine what the terms of the suspension require of them; (3) on probable cause of imminent risk of death or serious injury, emergency suspension ex parte, with a post-deprivation hearing within [10] days; (4) disqualification from acting as a controlling person of any covered system; and (5) suspension and debarment modelled on FAR subpart 9.4.

(e) Access and demand. The Agency and the Attorney General may, upon reasonable notice and during ordinary business hours, require any person subject to this Act to produce for inspection, verification, and copying any record required to be established, maintained, or preserved under SEC. 12 or by rule under SEC. 3, and may require a written response, under oath, to interrogatories reasonably related to the existence, location, custody, and completeness of such records. A demand shall be in writing, shall identify the records sought with reasonable particularity, and shall state the provision of this Act to which they relate. On petition of the person served, [the court of general jurisdiction of the county in which the Agency sits] may quash or modify a demand that is unreasonable or oppressive; on petition of the Attorney General, that court may enforce it. A demand under this subsection is a lawful demand for purposes of SEC. 5(f). Nothing in this subsection authorizes entry upon premises, or access to any material, beyond what is reasonably necessary to obtain the records demanded.

(f) No substitution, and no lesser penalty by reason of office.

(1) A prosecution under this Act does not bar, and is not an alternative to, a prosecution under the general criminal law of this State for the same conduct. Where the same conduct constitutes an offense under this Act and an offense under the general law carrying a longer term or larger fine, the availability of this Act is not a ground for charging the lesser, and a sentence under this Act is not a ground for a lesser sentence under the other.

(2) The liability of an entity under this Act is not an alternative to, and does not satisfy, discharge, mitigate, or bar the liability of any natural person under SEC. 6. A payment, penalty, settlement, or judgment made or borne by an entity is not a factor in mitigation of any sentence imposed on a natural person under this Act, and shall not be considered as one.

(3) No agreement to defer or to decline prosecution, and no diversion, may resolve the liability of a natural person under SEC. 6 except upon the approval of the court, granted on the record after a statement of reasons by the Attorney General, and the court shall consider whether the agreement would leave the person's conduct answered only by a payment borne by another.

(4) A term of imprisonment imposed under this Act shall not be suspended in whole, nor converted to a fine, by reason of the payment of any penalty, restitution, or disgorgement by any person.

(5) Presumption of a custodial sentence in the enhanced tier. Upon conviction under SEC. 6(b) the court shall impose a term of imprisonment unless it states on the record substantial and compelling reasons for not doing so. In deciding whether such reasons exist the court shall have regard to the extent of the authority the person held, the benefit derived by the person and by any entity from the violation, whether the person acted after notice of the matter, and whether a sentence without custody would leave the person's conduct answered only by money paid by another. A statement that the person is of previous good character, holds a position of responsibility, or has made or procured a payment is not by itself a substantial and compelling reason.

(6) The court shall state on the record its reasons for the sentence imposed under SEC. 6,

whether or not custody is ordered.

(g) The Attorney General enforces this Act. Corporate payment of any penalty imposed on a natural person does not extinguish individual liability, does not reduce any term of imprisonment, and is a violation of SEC. 7(b).

(h) Fund. The [Frontier Systems Accountability Fund] is established. All penalties, fines, disgorgement, and other monetary recoveries under this Act, after satisfaction of restitution, shall be deposited in the fund; awards under SEC. 11 are paid from it; the balance [is appropriated to the Agency's functions under this Act / reverts to the general fund, at the adopting state's election]. The fund continues in operation, fed by every source not suspended or invalidated, notwithstanding the suspension or invalidity of any single provision of this section.

SEC. 11. WHISTLEBLOWERS

(a) Award. A person who voluntarily provides the Agency with original information leading to a successful enforcement action under this Act in which monetary sanctions exceed $[1,000,000] shall receive not less than 10 and not more than 30 percent of the sanctions collected, per the structure of 15 U.S.C. § 78u-6. Where the information leads to a successful enforcement action in which monetary sanctions do not exceed that sum, or to a conviction under SEC. 6 in which no monetary sanction is imposed, the Agency shall pay an award of not less than $[250,000] from the fund established by SEC. 10(h), and an award under this sentence is not reduced by reason of the absence or smallness of a monetary sanction. A conviction under SEC. 6 is a successful enforcement action for the purposes of this section.

Awards are paid from the fund established by SEC. 10(h). Awards remain payable from the fund whatever the source of the amounts in it; the suspension or invalidity of SEC. 10(a) does not suspend this section.

(b) A report may be made anonymously through counsel; the Agency shall protect the reporting person's identity, including in any award.

(c) No person may take any action to impede an individual from communicating with the Agency concerning a possible violation of this Act; any agreement or condition purporting to do so is void.

(d) Retaliation. (1) No person shall discharge, demote, suspend, harass, blacklist, withdraw or decline to renew an engagement, report to a licensing or immigration authority, threaten, or in any other manner discriminate against another person because that person has made, or is believed to have made or to be about to make, a report of the kind described in this section, or has assisted or is believed likely to assist in an inquiry under this Act. Retaliation gives rise to a civil action for reinstatement, double back pay, and fees. (2) A controlling person who directs retaliation prohibited by paragraph (1), or who, having authority to prevent or correct it, knowingly permits it to continue, commits an offense punishable under SEC. 10(b); and where the retaliation is directed at a person who has reported a matter concerning a risk of death or serious injury, the offense is within SEC. 6(b). (3) This section protects an employee, a former employee, an applicant for employment, an officer, a director, a contractor, a subcontractor, an agent, and an employee of any of them, without regard to the person's position, seniority, or place of work, and without regard to whether the matter reported is within the scope of that person's duties. (4) A report is protected whether made to the Agency, to the Attorney General, to a law enforcement officer, to a court, to a person within the entity having authority to inquire into or correct the matter, or to a controlling person; and a person is not required to report internally before reporting to the Agency, nor to notify the entity that he has done so. (5) No agreement, policy, contractual term, condition of employment, severance term, settlement, release, or arbitration provision may waive, limit, or condition any right under this section, may require notice to any person before a report is made, may require the reporting person to withdraw or disavow a report, or may require the return or destruction of any document lawfully obtained and provided to the Agency. Any such term is void to that extent, and a person who proposes such a term knowing its effect commits an offense punishable under SEC. 10(b). (6) A person who has participated in a violation and who reports it is not thereby relieved of liability, but the report and the extent of the person's cooperation shall be considered in mitigation, and the Agency may reduce or remit an award to that person to the extent of the person's own culpability. Nothing in this paragraph confers immunity. (7) In an action under this section, proof that a protected report was made and that adverse action followed within [one] year raises a rebuttable presumption in a civil proceeding that the adverse action was taken because of the report; in a criminal proceeding those facts operate as a permissive inference only. The presumption is rebutted by clear and convincing evidence that the same action would have been taken for the same reasons in the absence of the report.

(e) The Agency shall act upon, or publish a reasoned declination of, any credible report within [180] days. (f) Rules under SEC. 3 shall provide for the handling of security-sensitive information in reports and awards.

SEC. 12. MACHINERY

This Act takes effect [90] days after enactment; until the Agency is designated and organized to receive them, transmission to the Attorney General satisfies any requirement under this Act of transmission to the Agency, and the Attorney General shall transfer the materials to the Agency upon its organization; duties and offenses commence as provided by SEC. 3(c); [180-day] transition for covered systems deployed before the commencement applicable to them under SEC. 3(c), running from that commencement; no retroactive liability; records sufficient for audit (version identifiers, compute records, evaluation results, tool and permission manifests, change histories, and the compensation records upon which SEC. 7(a) operates) retained for [ten] years from creation; and, separately from the data underlying them, every finding, result, conclusion, or recommendation concerning the safety or security of a covered system that was made, recorded, or communicated within the entity, together with each version of any document in which it appeared and a record of any material alteration to or removal of it, retained for the same period. Where a retention or deletion schedule applicable to underlying data would otherwise cause a finding to become unrecoverable, this sentence operates independently of that schedule, and compliance with such a schedule is not a defense to the loss of a finding; or for [five] years after the covered system last operates in or is last deployed in or into this State, whichever period ends later; and, from the time the entity or any controlling person has notice of a critical safety incident, of an investigation, or of a proceeding under this Act to which the records are reasonably relevant, the records shall be preserved until the conclusion thereof; confidentiality of reported material as follows: reports under SEC. 9, certifications under SEC. 8, and validation materials under SEC. 3 are exempt from disclosure under [the State public-records act], and to the extent they contain security-sensitive information — including information that would materially assist unauthorized access to model weights or covered systems — shall be maintained under seal in any proceeding; this exemption does not limit access by the Agency, the Attorney General, or a court under seal, does not exempt any person from any obligation to disclose under any other law, does not create any privilege for underlying facts, which remain subject to discovery and subpoena from any source, and does not restrict any use of any material in an enforcement proceeding under this Act. Dissolution, merger, conversion, division, or reorganization of an entity does not abate any proceeding or extinguish any liability under this Act; a surviving, resulting, or successor entity, and any entity that acquires substantially all of a covered entity's assets and continues its business, assumes the predecessor's liabilities under this Act; nothing in this section transfers the criminal liability of any natural person to any other person. A prosecution under this Act shall be commenced within [five] years after the violation; for a continuing violation, within [five] years after its last day; where the violation was concealed by an affirmative act, within [five] years after its discovery by the Agency or the Attorney General; where an incident or matter concerning the violation was required to be reported under SEC. 9 and was not reported as that section requires, within [five] years after its discovery by the Agency or the Attorney General, the failure to report being a concealment for the purposes of this sentence whether or not any further act was done; where a record required by this section was not created, was not retained, or was not produced upon lawful demand, within [five] years after its discovery by the Agency or the Attorney General; and a prosecution for an offense to which SEC. 10(c)(2) applies may be commenced within [ten] years.

This Act shall be construed to reach the persons with the greatest practical power over covered systems; it shall not be construed to permit the discharge of any person's liability through the liability of another. Nothing in this Act displaces any other remedy of this State.

SEC. 13. SEVERABILITY, CONFORMING OPERATION, AND REVIVAL

(a) Severability. The provisions of this Act are severable. If any provision, or any application of any provision to any person, capacity, class of persons, or circumstance, is held invalid or unenforceable, the holding does not affect any other provision or application that can be given effect without it, and this Act shall be construed and enforced to the maximum extent it may lawfully operate.

(b) Order of severance. Where a court can preserve the operation of this Act by severing a narrower provision or application rather than a broader one, it shall do so, and shall sever later-listed matter before earlier-listed matter:

(1) First rank. The offenses under SEC. 5(b) and SEC. 5(d); the offense under SEC. 5(a) as applied to the deployment (otherwise than by release), material expansion, or continued operation of a covered system in or into this State; SEC. 4 and SEC. 6; the remedies and penalties of SEC. 7 and SEC. 10(b) through (h) as applied to those offenses, and SEC. 10(a) as applied to those offenses; the duties of SEC. 2 as applied to a person in that person's capacity as a provider or deployer; and SEC. 1, SEC. 3(a), SEC. 3(c), and the provisions of SEC. 12 governing limitations, transition, retroactivity, and successor liability.

(2) Second rank. SEC. 11; the remaining provisions of SEC. 12; the offenses under SEC. 5(e) and SEC. 5(f), except as provided in paragraph (3).

(3) Third rank. The duties of SEC. 2 and SEC. 3 as applied to a person in that person's capacity as a developer, including pre-release evaluation and weight security; the application of SEC. 1(c) to development, training, evaluation, or testing conducted outside this State; SEC. 5(a) as applied to a release; SEC. 5(f) as applied to records of pre-release evaluation held by a person in that person's capacity as a developer; the validation modes of SEC. 3(b) requiring assessment by a person other than the developer.

(4) Fourth rank. SEC. 8; SEC. 9; SEC. 5(c).

(5) Preservation of elements. No provision shall be severed to an extent that deprives a surviving offense of an element, a definition, a standard, a limitations period, or a commencement condition on which that offense depends. A provision of a later rank that supplies such matter to an offense of an earlier rank continues in effect for that purpose notwithstanding its severance for every other purpose. In particular, SEC. 3(a) and SEC. 3(c) continue in effect to supply the content of, and the commencement condition for, any surviving offense under SEC. 5. The civil penalty of SEC. 10(a) and the criminal penalties of SEC. 10(b) and (c) sever independently of one another; the invalidity or suspension of either, in whole or as applied, does not affect the other; and the fund under SEC. 10(h) continues in operation whatever else is severed, fed by the sources that remain. The offense under SEC. 5(f) and the duties of SEC. 12 sever independently of one another: severance or suspension of the offense leaves the duties enforceable under SEC. 10(a), and severance of any reporting or certification duty does not sever the records duties or the offense that enforces them.

(6) Declared intent. The Legislature declares that it would have enacted the provisions of each rank irrespective of the invalidity of any later rank, and specifically that it would have enacted the first rank, together with the matter preserved to it by paragraph (5), had it known that no later rank could take effect.

(c) Conforming operation. (1) The Attorney General shall, by order published in [the State register], determine whether and to what extent any Act of Congress, or any regulation having the force of law, preempts the application of any provision of this Act. Upon publication, the provision is suspended to the extent, and only to the extent, stated in the order. A provision is suspended under this subsection only by such an order, or by a final judgment no longer subject to appeal in a proceeding to which this State was a party; and a suspension applies only to conduct occurring after the date of publication of the order or of notice of the judgment.

(2) In making a determination under paragraph (1), the Attorney General shall preserve the operation of this Act to the greatest extent lawfully available, and shall have regard to the following, which are stated as directions to the Attorney General and not as conditions of any person's liability:

(A) where the federal enactment conditions the preservation of State authority upon the absence of obligations imposed on developers with respect to the development, training, evaluation, or release of a model, the order shall suspend the duties of this Act as applied to persons in the capacity of a developer with respect to those matters, and shall preserve them as to every other person, capacity, and matter;

(B) where the federal enactment reaches only laws regulating conduct prior to deployment, the order shall preserve this Act as applied to conduct occurring upon or after deployment;

(C) where the federal enactment reaches a duty to report or to certify to the Agency, the order shall preserve the obligation, under SEC. 12, to create and retain the records that would have supported the report or certification, and those records shall be produced upon lawful process; an order preserving the obligation preserves the offense under SEC. 5(f) with respect to it; and

(D) where the federal enactment reaches only laws that target developers of artificial intelligence models, the order shall so state, and nothing in this Act limits the application to any person of the generally applicable criminal law of this State, including the law of homicide, reckless endangerment, endangerment by unsafe or adulterated goods, and false statement to a public officer, which applies to conduct concerning covered systems as it applies to all other conduct.

(3) No person may be convicted of an offense under this Act for conduct occurring during a period in which the provision creating the offense stood suspended under this subsection.

(4) Review of an order. An order under paragraph (1) is subject to review on the petition of any person, and the Attorney General shall reconsider an order upon the petition of any person presenting grounds to believe that the federal enactment stated in it does not preempt the provision, or does not preempt it to the extent stated. The Attorney General shall, within [90] days of such a petition, publish either an order terminating or narrowing the suspension or a reasoned refusal, and a refusal shall state the grounds

relied upon. Nothing in this paragraph makes the validity of a suspension a condition of any person's liability, and no failure to act under this paragraph creates a defense to any offense under this Act.

(d) Revival. A provision suspended under subsection (c) is not repealed. The Attorney General shall, within [30] days after the expiration, sunset, non-reauthorization, repeal, or judicial invalidation of the federal enactment stated in the order, or after a final judgment no longer subject to appeal determining that the enactment does not preempt the provision, publish an order terminating the suspension. The provision resumes operation on the date of publication of that order and applies to conduct occurring on or after that date. No person is liable under a provision for conduct occurring before that date.

(e) No inference. A suspension under subsection (c) is not evidence that the suspended provision was invalid, and does not affect liability for conduct occurring before the suspension took effect.

(f) Character of this Act. This Act is an exercise of this State's police power to punish conduct that endangers persons and property within it. Its offenses are offenses of general application in the sense that they punish the causing of, and the failure to exercise due care against, dangers of a kind this State punishes generally: the endangerment of the public by unsafe goods, the obtaining of unauthorized access to the property of another, the making of false statements to public officers, and the destruction or falsification of records. It does not license, permit, approve, register, or certify any person, product, or activity; it does not condition any deployment, expansion, or release upon the approval of any officer of this State; it imposes no requirement that any person express, adopt, or refrain from expressing any opinion; and it neither regulates nor prescribes the development, training, or design of any model except as SEC. 1(c) provides in relation to a deployment in or into this State.

(g) Construction against partial adoption. This Act's central elements are: (1) duties owed by an identified natural person holding practical power, and not by an entity alone; (2) the non-delegation rule of SEC. 4(e); (3) a criminal floor at SEC. 6 rather than a schedule of civil penalties; (4) personal certification under SEC. 8; and (5) the records duties of SEC. 12. An enactment adopting this Act's definitions, thresholds, reporting periods, or framework language while omitting any of those five is not an enactment of this Act, and this section shall not be construed to suggest otherwise.
