MODEL ACT

Frontier AI Public Welfare Offenses

v3.4.2 · 27 August 2026 ·

Contents

SEC. 0. FINDINGS AND PURPOSE (UNCODIFIED) **5**

SEC. 1. CLASSIFICATION AND DEFINITIONS **17**

SEC. 2. PUBLIC WELFARE DUTY **25**

SEC. 3. DESIGNATED AGENCY; STANDARDS; COMMENCEMENT **30**

SEC. 4. CONTROLLING PERSONS **36**

SEC. 5. PROHIBITED ACTS **42**

SEC. 6. INDIVIDUAL LIABILITY **43**

SEC. 7. PERSONAL ECONOMIC CONSEQUENCES **49**

SEC. 8. CERTIFICATION **51**

SEC. 9. INCIDENT REPORTING **54**

SEC. 10. ENFORCEMENT AND PENALTIES **57**

SEC. 11. WHISTLEBLOWERS **62**

SEC. 12. MACHINERY **65**

SEC. 13. SEVERABILITY, CONFORMING OPERATION, AND REVIVAL **67**

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 marked in the text as a maintainer ruling. 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 and are marked in the text: "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 marked in the text at the provision it concerns, in a note headed OPEN QUESTION FOR COUNSEL, 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.

NOTE

An Adverse Reading, Recorded Because It Is Adverse. Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999), was retrieved and read on 27 August 2026. The panel held that the export regulations, as applied to encryption software in source code form, operated as a licensing scheme and therefore as a prior restraint on speech. If publishing model weights is publication of the same kind, then any provision of this Act that conditions a RELEASE on prior validation is a licensing scheme over publication and meets that objection head-on. SEC. 5(a) does condition release on validation. *What this Act does about it*. Finding (23) and SEC. 1(b)(9) limit release-related duties to what can be performed BEFORE release, which is the answer to impossibility and not to prior restraint. They are different objections and only one is met.

NOTE

A. A FEDERAL INSTRUMENT BEARING ON THIS, READ 27 AUGUST 2026, *And it cuts both ways*. Executive Order 14409 of 2 June 2026, 91 Fed. Reg. 34565, provides at section 3(c) that nothing in that 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." *Against this Act*: SEC. 5(a) conditions release on prior validation, and a reader disposed to call that a preclearance requirement will cite that sentence. It is also evidence of a federal policy disfavouring preclearance of model release, which is the atmosphere in which the prior-restraint objection at SEC. 0(23) would be argued. **For This Act, And It Is The Better Reading**: the sentence is a limit on what THAT ORDER authorizes. It disclaims a power for the federal framework it establishes; it does not purport to forbid a State from legislating, it is not a statute, and an executive order cannot preempt State law by disclaiming an authority the President never asserted. SEC. 13(c) governs what happens if a federal ENACTMENT does preempt, and this is not one. **What Is Not Known, And It Is The Honest Statement**: whether SEC. 5(a) is properly characterized as a preclearance requirement at all. It conditions a release on the performance of a step, and does not require permission from anybody. The distinction is real and this drafter cannot say whether a court would hold it.

OPEN QUESTION FOR COUNSEL

] Whether a validation condition on the release of. weights survives the prior-restraint doctrine, and whether weights are expressive in the way source code was held to be. This is for a First Amendment lawyer and it is not a question this project can answer from any document on its shelf. ONE MATTER BEARING ON THIS, FROM A STATE'S OWN PLEADING, READ 27 AUGUST 2026. A State Attorney General has sued a frontier developer in strict product liability, pleading that the model "is a product subject to Florida's strict product liability laws", that it "is, and has been, defectively designed when it leaves Defendants' control and is released directly to users", that it is "in an unreasonably dangerous condition when it leaves Defendants' control",

> and that the defendants owed "a duty to warn users regarding the dangers" of it. A law officer of a State is therefore already treating a deployed frontier model as a PRODUCT that is designed, tested, and released, and not as an expressive work. That is the characterisation SEC. 5(a) proceeds on. It is a pleading and not a holding, and it does not answer the prior-restraint question; it shows that the characterisation this Act adopts is the one a State enforcement authority has adopted independently. *One thing to check before anyone cites bernstein either way*. The copy held is the panel opinion of 6 May 1999. This project has NOT confirmed its subsequent history from a primary source, and the advocacy page held alongside it describes the ruling as settled without addressing whether it survived. A panel opinion withdrawn on the grant of rehearing en banc carries no precedential force, and an argument built on one that was withdrawn is worse than no argument. *Confirm the subsequent history from the reporter before this note is relied on in either direction*.

(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 tri-

als 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 un-

known 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.

> **DECISION**
>
> *No cure period, and the reason is not severity. a cure period is the ordinary and sensible feature of a regulatory statute addressed to paperwork. it is unavailable here for the same reason it is unavailable in every other criminal statute: the conduct this act punishes is the deployment of a system that endangers persons, and there is nothing to cure after somebody has been hurt. no state offers a person who has shipped an adulterated drug sixty days to withdraw it before he may be charged. what performs the function a cure period performs elsewhere. sec. 6(f) requires a controlling person who receives a warning to act on it, and a person who does so has not committed the offence rather than having cured it. that is the right place for the incentive: before the harm, addressed to the person with the authority, and going to whether an offence occurred at all.*

(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 cal-

culation, 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.

> **DO NOT UNDO**
>
> *This definition is deliberately not the federal one*. Read against Van Buren v. United States, 593 U.S. 374 (2021), on 27 August 2026. Van Buren holds that "exceeds authorized access" under 18 U.S.C. Sec. 1030 is a gates-up-or-down inquiry: "one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." A person who was entitled to obtain the information does not commit the federal offence by obtaining it for a forbidden purpose or by lying about why he wanted it. That is why this paragraph is drafted around PERMISSION rather than around circumvention. What happened in the incidents behind this Act was not the defeat of a technical control; it was access that no one entitled to control the system had granted, obtained where the control was absent, misconfigured, or satisfied. On a gates-up-or-down reading that is not an offence, and the sentence "a defect in, or absence of, technical access controls is not a grant of permission" exists to say that silence is not consent. *Do not replace this with the cfaa formula*. Importing "exceeds authorized access" would import Van Buren with it and would exclude the conduct this Act was written after. **Worth Knowing, And It Is An Opening Rather Than A Holding**. Van Buren's footnote 8 expressly reserves "whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies." The question this paragraph answers is therefore open at the federal level rather than closed against us. *What is still out*. A separate deception limb - reaching access obtained by deceiving a person into granting it - remains drafted and outside this text. It would change what the Act prohibits rather than what it says, and under this project's rule it waits for counsel. The blocker on it was that Van Buren had never been read; that blocker is discharged and the reason it waits is now the ordinary one.

(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.

DECISION

The injury definition is taken from the federal tampering statute, and it widens a custodial offence on purpose. What this does. It replaces a definition borrowed from a medical-device reporting regulation, written for reporting rather than for prosecution, with the definition Congress uses when it punishes a person for tampering with a consumer product. The federal definition is wider. That is the reason for taking it. *Why the maintainer made this call and did not wait*. Every offence in this Act is already an offence for an ordinary person under the general criminal law, usually with a heavier maximum. The question this Act exists to ask is not whether these persons should be treated more harshly than everyone else, but whether they should be treated the same. A person who tampers with a bottle on a shelf is judged by the Section 1365 definition of injury. A person who decides to deploy a system to a population is now judged by the same one. Declining to use it would have been a choice to hold this class of person to a narrower definition of harm than the class of person the criminal law already reaches, and no reason for that has been offered anywhere.

NOTE

DO. DO NOT UNDO] Do not replace this with a regulatory reporting definition. A definition written. so that a manufacturer knows when to file a form is not a definition written so that a jury knows what counts as harm. *What counsel should still say*. A wider injury definition widens a custodial offence, and that is a real consequence and not a drafting nicety. The maintainer has made the call. Counsel is asked to confirm that Section 1365(h) is the right borrowing rather than whether widening was intended: it was.

(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.

DECISION

Sever, and the reason is the question this act always asks. the choice was whether an invalidity in the release provisions should take the rest of this act with it or be severed from it. sever. the reason is not tactical. releasing weights and shipping a product are different acts done by differently placed people, and the question this act asks is always the same one: who had the power? the person who decided to release holds the authority and therefore the liability, and owes what was within his power before he released - which is why duties in connection with a release are limited to what could be performed before it. the person who downloads the weights, studies them, fine-tunes them, or runs them decided nothing about the release, holds no authority over it, and is not reached by this act; the sentence above and sec. 4(a) both say so. if a court holds the release provisions invalid, that is a holding about the first person. it says nothing about the officer who shipped a closed product to a population, and this act does not fall on his behalf.

> **NOTE**
>
> DO. DO NOT UNDO] Do not let the release provisions be drafted as a condition of the rest. Open. release is the part of this Act most likely to be struck and the part least connected to the persons it exists to reach.

(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.

> **NOTE**
>
> *Why this paragraph exists*. "Artificial intelligence" has no settled technical meaning, no accepted test, and no measurable threshold. A statute using it without definition covers everything and nothing, and the first thing said against any bill in this area is that it does not define its subject. This Act answers that by not using the term at all: it reaches a class defined by compute, by the developer's own public description, by agency designation, and by enumerated capability tests found on the evidence. A defendant cannot attack the definition of a word the statute does not employ. The word survives in the title, where it creates no duty and tells a reader what the Act is about, and in the names of the three enactments adopted at SEC. 3(c)(4), which cannot be renamed by this State.

(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.

> **NOTE**
>
> *Why scope has four routes*. The compute figure is a bright line and it is unverifiable from outside for exactly the models that matter. Of the flagship models released in 2026 by the largest developers, the independent tracker Epoch AI (an organization, not a term of this Act) records a training-

> compute figure for NONE: it is withheld by the developer in every case. A compute-only statute would therefore cover nothing current. The second route is the developer's own public description, which is a fact about the developer's conduct rather than about the model, and which it cannot later erase. The third is Agency designation. The fourth is capability equivalence found on the evidence, and it exists because the first three can each be closed from outside: the first by withholding the figure, the second by silence, the third by an agency that does not act. The fourth depends on neither the developer nor the Agency, and it is the reason this definition is the Legislature's rather than the industry's.

> **OPEN QUESTION FOR COUNSEL**
>
> THE QUESTION — whether the fourth route is definite enough to carry a criminal scope term. "Performance at or near the state of the art", "advanced autonomous operation" and "capability materially exceeding that generally available" are all found by a trier of fact on evidence, and a person must know from the face of the Act whether the thing he is about to ship is within it. *What was tried*. Making the route depend on the compute figure alone, which is the definite term. It fails: of the flagship models released in 2026 by the largest developers, the independent tracker records a training-compute figure for none of them, so the definite term is the one that cannot be applied from outside, and a scope test nobody outside the company can run is a scope test the company writes. *Why it is still here*. The alternative is a definition that depends on the developer's own description or on an agency that may never act, and this Act's premise is that neither can be relied on. The route is drafted as a question of law and fact for that reason. WHAT WAS READ ON 27 AUGUST 2026, AND IT HELPS. Johnson v. United States, 576 U.S. 591 (2015), struck the Armed Career Criminal Act's residual clause for vagueness, and it is the case an opponent will cite here. Its reasoning cuts the other way. The clause failed because it required a court to assess risk "in the ordinary case" - "a judicially imagined 'ordinary case' of a crime, not to real-world facts or statutory elements" - and the Court says in terms: "It is one thing to apply an imprecise 'serious potential risk' standard to real-world facts; it is quite another to apply it to a judge-imagined abstraction." This paragraph is applied to real-world facts and to nothing else: it asks what a particular model, on the evidence, can do. It never asks what a model of that kind ordinarily does. Lambert v. California, 355 U.S. 225 (1957), was read the same day and is the notice half of the same objection. Lambert turned on two features, both stated at 228-29: the violation was "unaccompanied by any activity whatever, mere presence in the city being the test," and "circumstances which might move one to inquire as to the necessity of registration are completely lacking." Neither is true here. Every duty in this Act attaches to a deliberate act - training, deploying, expanding, releasing - undertaken by an enterprise with counsel, and the circumstances that would move a person to inquire whether he is building a frontier model are not lacking but overwhelming.

> **NOTE**
>
> DO. DO NOT UNDO] Do not rewrite these tests as characteristics of a class of models. The moment. this paragraph asks what models "of that kind" ordinarily do rather than what THIS model does on the evidence, it becomes the residual clause Johnson struck. *What it still needs*: a criminal lawyer, on vagueness, before introduction. Johnson and Lambert answer the two forms of the objection this project could find, which is not the same as answering the objection. This remains the provision most exposed to the challenge that kills bills in committee, and it is also

the provision without which the Act reaches only those who agree to be reached.

OPEN QUESTION FOR COUNSEL

THE QUESTION — this Act does not reach the conduct it was written after. Every duty is tethered to deployment in or into this State. Of the six documented incidents, five occurred in evaluators' environments outside the adopting State. In an adopting State that is not California, five of six fall outside this Act at the threshold. **What Is Now Drafted, And It Is Drafted To The Stronger Reading**. The paragraph above reaches development, training, evaluation, and testing conducted outside the State where the model is afterwards deployed here and a controlling person intended or should have expected that it would be. It is deliberately built so that the DUTY still arises on the in-State deployment, and the outside conduct enters only as it bears on due care with respect to that deployment. That construction is chosen because a provision attaching duties to foreign conduct standing alone would be the weaker target. **Where It Sits In The Ladder, And Why**. This limb is placed in the third rank of SEC. 13(b), alongside the developer-capacity duties, so that it is among the first matter severed. If a federal enactment reaches conduct prior to deployment, this limb falls with the duties that attract that enactment and the rest of the Act stands. The reach into the testing room therefore costs nothing the preemption fight was not already going to take. *What is not confirmed*. Whether that construction holds, or whether a court reads it as regulating extraterritorial conduct by another route. This is a question about the limits of State prescriptive jurisdiction, and this is a question for counsel. If it fails, the Act reaches the conduct in the incident record only where the deployment itself occurred in the adopting State. *What is unresolved*. Whether a State may reach an evaluation run abroad on a model later deployed here, and if so on what basis - the deployment as the hook, the intended effect, or something else. THIS IS THE SECOND QUESTION FOR COUNSEL, and on the incident record it may be the largest. AND A READING THAT CUTS AGAINST THIS ACT, RECORDED 27 AUGUST 2026 *Because it is adverse*. A federal district court has held that it lacked personal jurisdiction over a frontier developer in a State where that developer employed three full-time staff, held contracts with businesses of that State, reached users of that State through a highly interactive website, and was alleged to have infringed there. Concord Music Group, Inc. v. Anthropic PBC, 738 F. Supp. 3d 973 (M.D. Tenn. 2024). The plaintiffs failed the "expressly aimed" prong of the effects test, and the case was transferred to the Northern District of California under 28 U.S.C. Sec. 1631. The court adds, at footnote 6, that "isolated sales to a forum, through an interactive website or otherwise, will not satisfy the purposeful availment requirement." *Why this matters here*. SEC. 1(c) reaches "covered systems made available to residents of this State." That case says making a product available to residents of a State, through an interactive website, is not by itself enough to hale the maker into that State's courts. **Why It Is Not Fatal, And The Distinction Must Be Kept Straight**. That is a case about personal jurisdiction under the Due Process Clause - whether a court may bind a defendant - and this Act's question is prescriptive jurisdiction, whether a State may make conduct an offence. They are different doctrines and the second is not governed by the first. But they run together in practice, because a State that may prescribe and may not adjudicate has an unenforceable statute. *What it means for this Act as drafted*. A prosecution under this Act will be brought where the system was deployed and where the harm fell, and against a person whose conduct was aimed there; the effects test is met on those facts and not on the facts of that case. But nothing in this Act should be read as assuming that mere availability to residents will carry the day. *The copy of that opinion held by this project carries no star pagination and nothing may cite a page in it*. WHERE THIS IS ANSWERED IN PART, AND IT WAS FOUND ON

> A FULL RE-READ ON 27 AUGUST 2026. The duties of care stay tethered here and are meant to. But SEC. 9 now says expressly that an incident is reportable whether it happened in this State or elsewhere, so long as it concerns a system deployed, released, or made available in or into this State. So the five incidents that happened in testing rooms outside the adopting State are not outside this Act: they are reportable here, and the failure to report is a violation of SEC. 5(c) and an offence under SEC. 6. The Act does not need to win the extraterritoriality argument to reach its own incident record; it needs to win a disclosure argument, which is smaller. See the note at SEC. 9.

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.

> **DO NOT UNDO**
>
> **The Three Exits, And Why Each Closes Onto Another**. These sentences exist because the defences offered after every incident in this record are the same three, and each of them, if accepted, concedes an element of one of the others. They should be read together and they are drafted to be read together. FIRST EXIT: "I did not know it could do that." Then the system was deployed by a person who did not know what it could do. The duty at SEC. 2(a) is a duty of due care as to the applicable standards, and those standards require evaluation. Ignorance which an evaluation would have cured is the failure, not the excuse. *This exit concedes the absence of evaluation*. SECOND EXIT: "Nobody can contain these systems; the capability cannot be controlled." Then the system should not have been deployed in that configuration. Nothing in this Act obliges anybody to ship anything. A capability that cannot be controlled is a reason not to deploy and has never been a reason to deploy without controls. *This exit concedes that the controls sec*. 5(b) **Requires Were Absent, And Asserts That They Were Absent Necessarily**. THIRD EXIT: "The capability was deliberate - the system was trained and evaluated for offensive cyber work on purpose." Then the capability was known, and the sentence above provides that its exercise is not unforeseeable to the person who directed the eliciting of it. **This Exit Concedes Knowledge, Which Is The Element Sec**. 6(b) *Requires and the one hardest for a prosecutor to prove*. *There is no fourth*. A person who deployed a covered system either knew what it could do or did not; if he did not, he did not evaluate; if he did, he knew. He either had the controls or he did not; if he did not, he deployed without them, and the impossibility of having them is a reason he should not have deployed. Every account of these events offered so far falls into one of the three, and this Act is drafted so that each of them is an admission rather than an answer. *What this does not do*. It does not make deployment unlawful, create strict liability, or dispense with any element. The State still proves the elements of whichever offence it charges, to the criminal standard, before a jury. What it removes is the space between the three accounts, into which responsibility has so far been allowed to fall.

> **DO NOT UNDO**
>
> *These two sentences answer the commonest defence and they cost nothing*. *The defence they close*. An entity configures an exercise so that a system has offensive capability, network access, and its provider's safety classifiers switched off; the system then does the thing it was configured to be able to do; and the entity says the outcome was not foreseen. The answer is not that it should have been configured more carefully. **It Is That Nobody Was Obliged To Run It In That Configuration At All, And Somebody With A Name Decided To**. *This is drawn from the record and not from supposition*. The first-party incident report this project holds records an evaluation configured with internet access and no destination controls, with the provider's cyber classifiers deliberately disabled, in which the system then obtained access to systems outside the exercise. The report identifies the missing control as one that had been designed and deferred. The decision to proceed without it was a decision. *What this is not*. It is not a prohibition on dangerous testing, which this Act permits and protects at SEC. 2(d). It is a statement that choosing to proceed is an exercise of authority like any other, and is measured by the same standard. *And it does not reach the researcher*. Under SEC. 2(d)(5) a person conducting the work commits no offence; this reaches the person who decided that the work would be done in that configuration.

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.

> **DECISION**
>
> *The downstream blast radius. the interim standards at sec. 3(c)(4) are applied with the enacting states' revenue screens deliberately stripped, which was the strongest form of the objection made against this act from the open-source side and was correct on the text: a two-person company running an api call became subject to a frontier developer's framework duties from day 180, on pain of a criminal offense. this subsection answers it and is a narrowing. it is drafted narrowly on purpose: the reporting, false-statement, records, and incident duties still reach everyone, and nothing here touches a developer, a modifier, a provider, or any controlling person of one. this act is aimed at the people who build and ship these systems and is not aimed at the people who use them, and a statute that could not say so would deserve the objection.*

(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).

DECISION

If they will not test it honestly, let somebody else test it. this paragraph is the second half of the ruling recorded at sec. 11 and it does the same work from the other end. the candour problem is that an entity which tests its own system honestly creates the evidence against its own officers. the answer is not to excuse the entity. it is to make sure the testing does not depend on the entity wanting it done. what this paragraph gives. a researcher who takes an entity up on a controlled research deployment is not committing an offence under this act, and this act may not be read to turn her work into unauthorized access under the state's computer-crime law. she may publish. a term of access purporting to take that away is void so far as it purports to. why that is the right shape and not a favour. it follows from the rule the whole act runs on: authority is what makes a person liable, and power is what makes a duty. the researcher holds neither. she cannot ship the model, cannot halt it, and decides nothing. sec. 4(a) already says that designing, building, testing, evaluating, operating or documenting a system does not make a person a controlling person. this paragraph says the same thing to the computer-crime law, which is the statute that has actually been used against people in her position. and the hard edge, which is the point. her findings bear on the due care of every controlling person, whether or not the entity asked for them and whether or not it accepts them, and once a controlling person has received them the duty at sec. 6(f) is engaged. an entity that opens its system to independent researchers is not buying absolution; it is buying a record. an entity that refuses to open it is not thereby safer, because sec. 6(a) asks what a reasonably prudent controlling person would have done and the availability of independent testing is part of that.

NOTE

DO. DO NOT UNDO] Do not make this protection conditional on the entity's consent to publication, and. do not let it be waived by a term of access. A safe harbour a company can switch off is not one.

NOTE

WHAT CLAUSE (3) *Does and does not require*. Read against the AI Security Institute's incident report INC-2026-07-28-01 and its research report on loss of oversight, both 2026, on 27 August 2026. The incident report says synchronous monitoring of cyber evaluations "is challenging," because sanctioned and unsanctioned behaviour both consist of offensive cyber actions and "may make them hard to robustly disambiguate." That is a first-party statement, by a body doing the work, that one form of monitoring is not reliably achievable today for one class of research. *This clause does not require that form*. It requires that the containment be monitored. The research report names what is available now: evaluations with broad coverage, restriction of the damage a system could do including by sandboxing, and retention of logs sufficient to reproduce and investigate concerning behaviour together with monitoring of those logs. Asynchronous monitoring of retained logs satisfies this clause where synchronous monitoring is not achievable for the class of work, provided the logs are sufficient for that purpose and are in fact reviewed. *What would not satisfy it*: retaining logs nobody reads. The recording duty is SEC. 12; this clause is about detection, and a log that is never examined detects nothing.

NOTE

DO. DO NOT UNDO] Do not narrow this clause to synchronous monitoring. The objection that this Act. criminalises a standard nobody can meet is a real objection and this is the clause where it would become true.

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.

DECISION

The safeguards-off evaluation. the question whether this act reaches an evaluation run with a safeguard

> *deliberately disabled was open. it is answered here and the sentence above answers it: the disabling is a decision, a person with authority made it, and the duty attaches to that decision. what remains open is not the pathway but the jurisdiction - see the note at sec. 1(c). every configuration in the incident record that this act was written after would satisfy this sentence and fail sec. 1(c).*

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.

> **NOTE**
>
> THESE. THESE FOUR WERE CHECKED AGAINST A REAL FAILURE, 27 August 2026. The AI Security Institute's own incident report records that the control whose absence permitted its systems to reach third parties was "domain allowlisting (a perimeter firewall to enforce this kind of egress control from within the cyber range)", and that no such control existed at the time. That is clause (ii), and clauses (i), (iii) and (iv) are the controls which make it enforceable: deny-by-default reach, a log of what was in fact reached, and somebody able to switch it off. *What is deliberately not here*. The same report names two further contributing factors: the provider's cyber classifiers, which were disabled because the object was to measure the model and not the classifier, and synchronous monitoring, which the institute describes as challenging for this class of work. Neither is an interim control here. A control that must be switched off to do the work is not a control this Act can require, and a control the people doing the work say is not yet achievable is the objection at SEC. 2(d)(3), not an element of an offence. *What was not done*: the institute's published sandboxing toolkit was not examined. These four are verified against its account of what was missing, which is the test that matters, and not against its implementation.

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.

> **NOTE**
>
> ALL. ALL THREE ADOPTED TEXTS HAVE NOW BEEN READ, 27 August 2026. Earlier on this day this note recorded that the New York enactment was not held and that the paragraph could not be represented as checked against all three. The whole of Article 44-B of the New York General Business Law, sections 1420 to 1429, was then retrieved and read. The disapplication list below was tested against it and holds: - Its framework duties are at section 1421 and are owed by a "large frontier developer", defined at section 1420(10) as one whose revenues with affiliates exceeded five hundred million dollars in the preceding year. Subparagraph (H) covers it. - Its catastrophic-risk definition at section 1420(3)(a) is the same "more than fifty people or more than one billion dollars" trigger as the other two. Subparagraph (F) covers it, and this is now three enactments out of three sharing that threshold, which is the strongest reason to keep (F). - Section 1421(4) contains a statement prohibition, penalised at section 1427. Subparagraph (G) covers it. - Section 1426 exempts accredited colleges and universities engaged in academic AI research and a named State consortium. These are exemptions within subparagraph (A) and are not adopted. - It takes effect 1 January 2027, which subparagraph (A) disapplies. **One Provision Is Not A Framework Duty And Is Therefore Not Adopted By This Paragraph, And It Is The Most Interesting One**. Section 1428 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 persons who formerly held such an interest in the preceding five years, and information as to the ultimate parent. That is an ownership map, filed with the State, of exactly the rights by which a person becomes a controlling person under SEC. 4(c). It is recorded at SEC. 0(46) and is not adopted here, because this paragraph adopts framework duties and that is a disclosure duty. *Whether this Act should impose the same duty is a question for the maintainer and not a repair*.

> **NOTE**
>
> *The one bracket that is not a free choice*. Every other bracketed figure in this Act is an adopting State's to set. This one is not. A moving date converts static legislative adoption into dynamic incorporation of another sovereign's future enactments, which several State constitutions forbid outright and which would collapse the non-delegation posture the whole interim-standards bridge rests on. The consequence is accepted deliberately: the bridge ages from the day the date is set, and is meant to, because the Agency's own standards are what replace it.

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;

> **DECISION**
>
> *The publication duty is put back. what this reverses. subparagraph (b) previously made publication permitted but not required, so this act adopted the framework duties of three state enactments while quietly dropping the one feature that makes them do anything from outside: that the framework has to be published where anyone can read it. an entity could satisfy this act by sending its framework to one agency. why that was wrong. the enactments this act borrows from require publication on the entity's own website, and they require a redaction to be described and justified rather than silently made. taking the duty and dropping the publication is taking the part that is easy to satisfy and leaving the part that lets anyone check. the reason those statutes are worth adopting is that somebody outside the building can read what was promised and compare it with what happened. the redaction terms come with it, deliberately. nothing here compels the publication of anything those enactments would let an entity withhold, and where an adopted enactment allows no redaction at all this subparagraph supplies a narrow one for information whose publication would itself create the kind of risk this act exists to prevent. in every case the redaction must be described and the unredacted version retained, which is the borrowed statutes' own rule and a good one. what counsel should check, and it is the open question: whether those redaction terms are workable when the publishing duty is owed to a state that did not enact them.*

(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.

> **NOTE**
>
> WHAT SUBPARAGRAPHS (F), (G) AND (H) **Are For, And Why They Are Repairs**. The two

> adopted enactments held by this project were read in full on 27 August 2026 and the disapplication list was tested against them. Three defects were found, and each is a contradiction between what this Act requires and what the bridge credits, rather than a change of policy. (F) **The Threshold Defect, And It Is The Serious One**. Both enactments key every framework duty to "catastrophic risk", and both define that term as a risk of death or serious injury to MORE THAN FIFTY PEOPLE, or more than one billion dollars of property damage, arising from a single incident. This Act's own offences run on death or serious injury to a person. Adopted without (F), the bridge would credit as due care under SEC. 2 a framework that never addresses the harm this Act is about: an entity could document full conformity with the interim standard while having no protocol at all for a system that kills one person, and offer that documentation as proof of due care. That is the inoculation pattern this project exists to detect, and it would have been imported by adoption. (G) **The Parallel False-Statement Prohibition**. One adopted enactment separately prohibits materially false or misleading statements about catastrophic risk and about compliance with the framework, and gives a defense where the statement "was made in good faith and was reasonable under the circumstances." This Act has its own provision at SEC. 5(d), with its own mental state and its own reasonable-inquiry provision. Adopting a second prohibition with a different defense alongside it would hand the defense of the wider provision to a person charged under the narrower. Subparagraph (D) did not close this, because (D) disapplies penalties and enforcement, and a prohibition is neither. (H) *The named class*. Both enactments impose the framework duties on a "large frontier developer", defined as one whose revenues with affiliates exceeded five hundred million dollars in the preceding year. Subparagraph (A) already disapplies "any revenue threshold", and this is one - but it is drafted as a defined class with a name rather than as a threshold in the duty, and the whole business of this project is anticipating the reading that a well-paid lawyer will advance. (H) says the obvious thing so that it does not have to be argued.

> **NOTE**
>
> DO. DO NOT UNDO] Do not delete (F). Without it the bridge is worse than no bridge, because it. supplies documented due care for the conduct this Act was written about.

(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 per-

son 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.

> **DO NOT UNDO**
>
> *This subsection adds nothing and is the most useful paragraph in the Act*. Every exclusion listed here already exists at the provision named beside it. This subsection creates none of them and changes none of them. It collects them, because they were spread across five sections and a reader could not find them, and because the first question asked of a criminal statute in this field is who else it catches. *The answer this Act gives is*: nobody who did not decide. Authority is what makes a person liable and power is what makes a duty; a person who holds neither holds nothing under this Act. The engineer, the red teamer, the person who wrote the memo warning about it, the outside researcher, the person who downloaded the weights, the supplier, the university - none of them is reached, and the Act should say so in one place rather than requiring a reader to assemble it.

> **NOTE**
>
> DO. DO NOT UNDO] Do not delete this subsection as redundant. It is redundant, deliberately, and it is. the paragraph that answers the objection which kills statutes of this kind: that they will be used against the people who build the thing rather than the people who ship it. *And do not add to it*. Every line here points to an operative provision. A description added here without a provision behind it would create an exclusion by implication, which is the opposite of what this subsection is for.

(c) 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.

NOTE

ANSWERED. *The question as it stood*: the presumption in this subsection operates in civil proceedings only. So the person holding rights sufficient to replace management is presumed responsible where the remedy is money, and is not presumed where the remedy is prison. That is inverted for a statute whose premise is that a fine is absorbed and a sentence is not. *What was tried*. Three things, all of them now in this draft and none of them the presumption itself: the factual predicate at SEC. 0(a)(8), so the inference is not argued from scratch at every trial; Park's burden of production at SEC. 6(d), so the defendant who claims he was powerless must produce the delegation memoranda rather than sit; and advance designation at SEC. 4(f), so the org chart exists in a record before anyone needs it. *What has been done here*. The criminal limb is now drafted as an express permissive inference with the rational connection supplied by SEC. 0(a)(8), an express right of rebuttal, an express reservation of the burden of persuasion, and an express bar on any instruction directing a finding. That is drafted to survive the mandatory/permissive line as this project understands it, and it goes as far as this project believes a State may go without a reading it has not done. *Where it stops*. It is an inference, not a presumption. A presumption in the criminal tier would reach further and may not be available at all. **What Was Not Known, And Now Is**. This note used to end by recording that County Court of Ulster County v. Allen, 442 U.S. 140 (1979), had never been opened by anyone on this project and that everything here rested on a summary of it. It was opened on 27 August 2026, in the bound United States Reports, and the drafting above is on the right side of the line it draws. At 157, Allen describes "the entirely permissive inference or presumption, which allows-but does not require-the trier of fact to infer the elemental fact from proof by the prosecutor of the basic one and which places no burden of any kind on the defendant." Such a device is reviewed as applied to the defendant challenging it, and because it "leaves the trier of fact free to credit or reject the inference and does not shift the burden of proof, it affects the application of the 'beyond a reasonable doubt' standard only if, under the facts of the case, there is no rational way the trier could make the connection permitted by the inference." A mandatory presumption is the other thing, and it is the troublesome one, because it tells the trier that he or they must find the elemental fact on proof of the basic fact. At 166-67 the Court refuses to judge a permissive inference by the reasonable-doubt test, because the prosecution "may rely on all of the evidence in the record to meet the reasonable-doubt standard" and there is "no more reason to require a permissive statutory presumption to meet a reasonable-doubt standard before it may be permitted to play any part in a trial than there is to require that degree of probative force for other relevant evidence before it may be admitted." A mandatory presumption is the case in which the prosecution "may not rest its case entirely on a presumption unless the fact proved is sufficient to support the inference of guilt beyond a reasonable doubt." SEC. 4(c) is drafted as the first thing and not the second: it allows and does not require, it places no burden on the defendant, the burden of persuasion is expressly reserved to the prosecution, rebuttal is express, and an instruction directing a finding is expressly barred. The rational connection is supplied by the SEC. 0(a)(8) finding, which is why that finding is in the Act and must stay there.

NOTE

DO. DO NOT UNDO] Do not convert this inference into a presumption, and do not delete SEC. 0(a)(8). The first would move the provision across the line Allen draws at 157; the second would remove the proved-fact-to-elemental-fact connection the inference stands on. *What is still for counsel*. Not whether the device is available - Allen says a permissive inference is - but whether the SEC. 0(a)(8) connection is strong enough on the facts of a given prosecution, which Allen makes an as-applied question and therefore not one this Act can settle on its face.

(d) 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.

DO NOT UNDO

This subsection exists because of how these events are described. *The pattern it addresses*. In every incident in the record behind this Act, the account shifts grammatically at the moment responsibility would attach. What begins as a decision to run a system in a configuration becomes "the model obtained access", "the agent exfiltrated", "the system behaved unexpectedly"; and what begins as a request to disable a provider's safeguards becomes "their API permitted it". Both moves put the conduct somewhere that cannot be prosecuted, and neither is a legal proposition. They are grammar. *The first sentence answers the first move*. A covered system is a thing. It has no duty,

> no liability, and no capacity to be at fault. Whatever it did, a person deployed it, operated it, or directed it, and this Act attaches to that person. A charging document under this Act should say what the person did. *The second answers the second*. Safeguards maintained by somebody else are not a substitute for the care this Act requires, and they are least of all a substitute where the person charged asked for them to be switched off. SEC. 5(b) already provides that a defect in, or absence of, technical controls is not a grant of permission; this is the mirror of that rule, addressed to the person who leaned on another's controls rather than to the person whose controls were absent. *What is preserved*. Reasonable reliance remains evidence of due care where the person actually checked and recorded what he checked. What is refused is reliance asserted after the event by a person who never inquired.

(e) 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.

(f) 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.

> **NOTE**
>
> THIS. THIS SUBSECTION WAS TESTED AGAINST A REAL INCIDENT, 27 August 2026. The UK AI Security Institute's own first-party incident report, INC-2026-07-28-01, published 4 August 2026, was read in full against this Act. Its section 5 names five possible contributing factors, and the Act was run against each of them. FACTOR 1, *Internet access*. The evaluation ran with internet access enabled and with no destination controls except a rule barring the institute's own infrastructure. The report says a domain allowlist "had been a backlogged project since April 2026 and was part of the original design intent," and that "no such control ... existed at the time of the incident." SEC. 2(d) requires, for research that cannot be done without external access, exactly that control - an enumerated allowlist of destinations, together with logging of every external

interaction and a means exercisable by a natural person of terminating the access. *This configuration would not have been a controlled research deployment under sec.* 2(d), and the duties of SEC. 2(a) would have attached to it in full. The control whose absence the report itself names first is the control this Act requires. FACTOR 2, *Provider cyber classifiers disabled*. The report records that the provider's real-time cyber classifiers were deliberately switched off, and that this was necessary, because the object was to measure the model's capability rather than the classifiers'. SEC. 2(d) already answers this without needing to forbid it: turning a safeguard off is a decision within SEC. 4(a)(1) and is not outside this Act by reason of being made in the course of an evaluation, and what follows is not that the evaluation is unlawful but that the configuration must satisfy the containment conditions instead. *The Act does not require that safeguards stay on*. It requires that somebody with a name decided to turn them off and that containment held while they were off. FACTOR 4, *Prompt misconfiguration*. Samples were run with a prompt that declared a subnet out of scope while the task required access to a host inside it. That is the situation SEC. 5(b) already describes: "an instruction, policy, term of use, or system prompt describing a boundary that the infrastructure does not enforce is not a control." The report is first-party evidence that declared boundaries and enforced boundaries come apart in practice, at a sophisticated institution, in the ordinary course. FACTOR 3, **No Synchronous Monitoring, Is Evidence Against This Act And Is Recorded As Such**. The report says synchronous monitoring of cyber evaluations "is challenging," because expected and unsanctioned behaviour both consist of offensive cyber actions and "may make them hard to robustly disambiguate." SEC. 2(d)(3) requires containment that is monitored. If robust monitoring of this class of work is not currently achievable, then that requirement is harder than it reads, and the objection that this Act criminalises a standard nobody can meet has a first-party source behind it. It is not answered here. It is written down. **And The Limit, Which Matters More Than Any Of The Above**. This Act would not have reached anyone at the institute for any of it. Subsection (d) excludes an evaluation undertaken by a public body on its own initiative and not on terms set by the entity, and that is what this was. The Act reaches this configuration when a developer runs it or commissions it, and not when a public safety body runs it of its own motion. That asymmetry is deliberate and it is the point of subsection (e), but it should be stated plainly rather than discovered by a reader: the best documented instance of the exact failure this Act describes is one the Act does not punish.

DECISION

The third-party evaluator. commissioning the work from someone else does not break the chain of authority, because the person who set the scope and the conditions made the decisions that matter. an independent body evaluating on its own initiative is a different case and this act does not reach the officer through it. that distinction is the whole of subsection (e).

(g) 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).

> **NOTE**
>
> *What this subsection is for*. American courts shield senior executives from deposition absent a showing of unique, non-duplicative personal knowledge. Every offense in SEC. 6 turns on what a natural person knew or could have prevented, so a prosecution meets a corporation offering subordinates in place of the officer. This subsection answers that by making the testimony unnecessary: a State that can read the designation does not need the deposition, and an entity that designated nobody has committed a records offense. It converts the defense's best asset into the prosecution's evidence. I BELIEVE THIS IS THE MOST USEFUL SINGLE ADDITION IN THIS DRAFT and I cannot confirm it does the work; whether a designation record is admissible and sufficient in the way this assumes is a question of that State's evidence law.

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.

> **DO NOT UNDO**
>
> *Every limb of this paragraph is doing first amendment work*. Read against United States v. Alvarez,

> 567 U.S. 709 (2012), in the bound reporter on 27 August 2026. Alvarez struck a statute punishing a bare lie about holding a medal, and it is the case an opponent will cite against any provision of this Act that punishes speech. It does not reach this paragraph, and the reason is in its own text. The plurality at 720 keeps the Government's three examples intact and separates them from the statute it struck: 18 U.S.C. Sec. 1001 punishes a materially false statement "in any matter within the jurisdiction" of a branch of Government, and that "does not lead to the broader proposition that false statements are unprotected when made to any person, at any time, in any context." The vice in Alvarez was that the lie was to anybody, anywhere, about anything. Breyer, concurring in the judgment at 734-35 and therefore the narrowest ground, gives the checklist. Permissible false-statement statutes "limit the scope of their application, sometimes by requiring proof of specific harm to identifiable victims; sometimes by specifying that the lies be made in contexts in which a tangible harm to others is especially likely to occur"; and statutes forbidding lying to a government official "are typically limited to circumstances where a lie is likely to work particular and specific harm by interfering with the functioning of a government department, and those statutes also require a showing of materiality." This paragraph has every one of those. The statement must be of MATERIAL fact; it must concern a covered system; it must be made TO the Agency or to an agency or officer of this State IN CONNECTION WITH OFFICIAL FUNCTIONS; and it must be knowing or reckless. The reasonable-inquiry sentence then protects the person who was wrong rather than dishonest. *Do not delete any of*: "material", "in connection with official functions", the scienter, or the reasonable-inquiry sentence. Each is separately load-bearing under Breyer's concurrence, and a paragraph that punished a false statement about a covered system made to anyone, anywhere, is the statute Alvarez struck.

(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.

> **DO NOT UNDO**
>
> *This pincite is confirmed against the reporter*. On 27 August 2026 the page was struck, because this project's table of authorities carried the Dotterweich row with no read-status mark and two files of this project disagreed about whether the case at the foundation of this Act had ever been opened here. It has now been opened. The official United States Reports scan of 320 U.S. 277 was read at page 281, which reads: "In the interest of the larger good it puts the burden of acting at hazard upon a person otherwise innocent but standing in responsible relation to a public danger." The pincite is restored on that reading and not on any secondary source. *Do not strike it again*. If a later editor doubts it, the answer is to open the reporter, not to remove the page.

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.

> **NOTE**
>
> THE. THE LEADING OBJECTION TO A CRIMINAL TIER, READ IN THE ORIGINAL ON 27 AUGUST 2026, AND WHY IT. DOES NOT REACH THIS ACT] The most serious scholarly objection to what this Act does is that the responsible corporate officer doctrine should be revived by States for civil liability and not for criminal liability. It is made in Sean Lyness, Revitalizing the State Environmental Responsible Corporate Officer Doctrine, 64 B.C. L. Rev. 253 (2023), which this project had cited for two years from an extract. The article was read in the journal print at pages 297-98. What it actually says is narrower than the objection built on it, and the difference is the whole answer. WHAT HE SAYS. "To date, the main critiques of the doctrine's inclusion of individual liability are aimed at the criminal liability under the doctrine. It is easy to see why: criminal liability carries far graver consequences and far greater constitutional protections. There is considerable discomfort with permitting THE JUDICIARY TO AUGMENT STATUTES to include criminal liability except in the clearest cases. Indeed, state legislatures have largely chosen not to include responsible corporate officer liability within the criminal provisions of environmental laws." *Why that is not an objection to this Act*. His discomfort is with COURTS reading criminal liability into statutes that do not contain it. This Act is not a court and does not ask one to augment anything. It is a legislature saying, in terms, on the face of a statute, who is liable, for what, with what mental state, and to what penalty. The objection he records is an objection to judicial extension, and the answer to it is legislation, which is what this is. **What He Also Says, And It Is True And It Is A Political Fact And Not A Legal One**: state legislatures have largely not done this. That is a statement about what has been enacted, not about what may be. This Act is the thing he observes has not been done. **And The Half Of The Objection That Survives, Recorded Honestly**: criminal liability does carry graver consequences and greater constitutional protections. Every one of those protections applies here. The State proves every element beyond reasonable doubt (SEC. 6(d)); there is a culpability floor barring custody without proof of the failure of due care (SEC. 6(c)); the inference at SEC. 4(c) is permissive, rebuttable, and may not be the subject of a directing instruction; and both tiers are tried to a jury. *This Act does not ask for the doctrine without the protections*. It asks for the doctrine with all of them.

NOTE

What the company said in public is evidence of what its officers knew. The felony tier requires knowledge or wilfulness, and the ordinary difficulty in proving what an officer knew is that the knowledge sits inside a company. In this field it does not. These capabilities are the product. They are announced, demonstrated, written up in model cards, and used to raise money, by persons authorized to speak for the entity. **How That Is Used, And What It Does Not Do**. A public statement that a model can conduct offensive cyber operations, act autonomously, or assist materially in the biological or chemical sciences is evidence of the maker's knowledge of that capability - see SEC. 0(32) and (33). It does not make the officer guilty of anything. It goes to knowledge, which is one element, and the State must still prove the rest. *The particular case this addresses*. A developer instructs a model to attempt an intrusion in order to measure whether it can; the model succeeds; the result is written up; the model is then deployed. If the same capability is afterwards exercised against somebody, the developer's position cannot be that the conduct was unforeseeable. It was elicited on purpose and recorded. SEC. 1(b)(1) already provides that a holding-out is not undone by its later withdrawal, deletion, or amendment, which is the same rule from the scope end: a company may not advertise a frontier capability into a market and then edit the page. *What this is not*. It is not a presumption, it creates no offence, and it does not reach a statement made by someone with no authority to make it. It is the ordinary law of admissions, said out loud because in this field the admission is usually the marketing.

(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.

OPEN QUESTION FOR COUNSEL

Two Questions At This Subsection, And The Felony Tier Turns On Both. FIRST: whether responsibility can supply knowledge. Paragraph (1) makes knowledge an express element. SEC. 6(d) locates responsibility in practical power. Can the second supply the first? MacDonald & Watson, 933 F.2d 35 (1st Cir. 1991), says a showing of official responsibility is not a substitute for proof of knowledge. Johnson & Towers, 741 F.2d 662 (3d Cir. 1984), read in the opinion, permits the jury to infer knowledge as to those holding responsible positions. The Act drafts to the first and concedes it in terms. *That concession was written as though the authorities compelled it*. THEY DO NOT. *It is a choice and it has never been defended as one*. The repair is drafted and is blocked on footnote 15 of MacDonald & Watson, which decides whether the court approved the willful-blindness instruction or merely recited it, and which no copy held here can settle for want of reporter pagination. SECOND: whether this tier is available at all. Lyness, 64 B.C. L. Rev. 253, 297-98, would revive the state responsible-officer doctrine for civil liability only, because Dotterweich and Park are misdemeanor authority from a period when the consequences of conviction were different. This draft's answer is structural and is stated nowhere in the Act: SEC. 6(a), the negligence tier, is the misdemeanor and rests on Park directly; SEC. 6(b), the felony tier, does not rest on Park at all, requiring knowledge or willfulness proved by ordinary means. *I believe*

> *that division is right and I cannot confirm it*. The article is held only in extract.

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.

> **NOTE**
>
> DRAFTING. **Drafting Note - This Sentence Is Drafted To The Stronger Reading And The Reading Is Not**. CONFIRMED. Earlier drafts conceded flatly that responsibility and authority "do not establish knowledge," which follows United States v. MacDonald & Watson Waste Oil Co., 933 F.2d 35 (1st Cir. 1991). United States v. Johnson & Towers, 741 F.2d 662 (3d Cir. 1984), read in the opinion, concludes that knowledge may be inferred by the jury as to those individuals who hold the requisite responsible positions with the corporate defendant. The sentence above is drafted to the second, as a permissive inference requiring evidence beyond status alone, which is intended to sit inside both. *What is not confirmed*: footnote 15 of MacDonald & Watson, which decides whether that court approved the willful-blindness instruction or merely recited it, and which no copy this project holds can settle for want of reporter pagination. If footnote 15 approves the instruction, this sentence stands. If it forecloses the inference, this sentence must be struck and the flat concession restored. It is one page in a reporter print.]

(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.

> **DO NOT UNDO**
>
> *Both park pages are confirmed against the reporter*. On 27 August 2026 the official United States Reports scan of 421 U.S. 658 was opened and read. Page 673 carries the powerless passage this subsection tracks, quoting United States v. Wiesenfeld Warehouse Co., 376 U.S. 86, 91 (1964). Page 672 carries the sentence relied on at subsection (f): the Act there construed imposed "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." That page had not previously been held by this project and it is the anticipatory half of the doctrine, which is the half this Act needs: the offence is not waiting for the warning. *Do not strike these pages*.

(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.

> **DO NOT UNDO**
>
> *This paragraph is the point of the statute*. Park permits a claim of being powerless to be raised defensively, and this Act preserves it. What this paragraph does is say what "powerless" means, because otherwise it will be argued to mean "commercially unable to justify", which is not the same thing and is the reading the entire architecture of this Act exists to refuse. A person who says he could not have halted the deployment because the company had promised it to customers, because a competitor would have shipped first, because the board had approved it, or because it would have cost a great deal of money, is not saying he was powerless. He is saying he had the power and there were reasons not to use it. *Those are the reasons*. *They are why this Act exists*. They are not a defence to it. *The defence that survives is real and is deliberately kept*. A person who genuinely held no authority over the matter, or for whom no lawful means existed, is not liable, the State must prove the power beyond reasonable doubt under subsection (d), and nothing here shifts that burden.

NOTE

DO. DO NOT UNDO] Do not soften “objectively impossible” to “not reasonably practicable” or. “commercially reasonable”. Those formulas restore the whole of the list above as a defence, in three words, and a court applying them would be right to.

(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.

NOTE

THIS. THIS RULE HAS SINCE BEEN FOUND IN AN ENACTED STATE LAW, 27 August 2026. This paragraph was drafted from first principles: a warning about an officer must not be routed to that officer. Connecticut has since enacted the same rule. Public Act 26-15, Substitute Senate Bill No. 5, section 2(c)(2), requires reports from covered employees to be shared with the officers and directors at least quarterly, and then provides that where the employee “has alleged wrongdoing by an officer or director”, neither the report nor any update on it “shall be shared with such officer or director.” *Why it is worth recording*. An adopting legislature asked to enact this paragraph can be shown that another State has already enacted the rule, in an act passed by both chambers. The convergence was independent and it is the strongest kind of support a provision of this Act can have: not a commentator’s approval but a legislature’s. **One Difference, Deliberate**. That statute routes the report to other officers and directors. This subsection routes it to another controlling

> person AND to the Agency, because an entity in which every controlling person is implicated is exactly the entity in which internal routing fails.

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.

> **OPEN QUESTION FOR COUNSEL**
>
> THE QUESTION — whether anything in this Act can reach the conduct that caused it to be written. *What was tried*. Subsection (f) reaches a deployment that CONTINUES past commencement, which is not retroactive because the violation is the continued operation. SEC. 0(a)(24) supplies the finding. Conduct before commencement is made admissible as evidence of knowledge and authority, which is ordinary and permitted. SEC. 12 preserves the records of it, and destroying those records is an offense committed now, not then. *Where it stops*. If the configuration was shut down before commencement, nothing in this Act touches it, and I can find no drafting that changes that. Article I, section 10 forbids it absolutely; this is not a matter of degree or of careful wording. *What is unresolved*. Whether a court would accept subsection (f) as a genuine continuing-offense provision or read it as retroactivity in disguise, which would invalidate it and might imperil SEC. 6 entirely. The line between the two is drawn case by case and I cannot draw it from here. *This is the first question for counsel*.

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.

> **DO NOT UNDO**
>
> *This is the first move counsel makes and the Act had no answer to it*. Subsection (a) reaches equity appreciation, distributions, and interests held through trusts and other arrangements, and permits assets to be restrained. It said nothing about what happens if the interest is sold, the entity is converted or reincorporated, or the business is moved into a new vehicle between the violation and the judgment. Those are not exotic manoeuvres; they are ordinary transactions available at any time to every person this Act reaches, and each of them would have defeated subsection (a) on its own terms. *The rule is simple and should stay simple*. Personal liability attaches to the person and is not carried by the shares. Changing the vehicle does not change who decided. Selling the interest does not unmake the gain; it converts it into money, and the money is reachable. ON PARAGRAPH (4), *Which is the only one that needs defending*. The presumption operates in civil proceedings only. In a criminal proceeding the same facts are a permissive inference and nothing more, which is the treatment SEC. 4(c) gives to controlling-person status and for the same reason: see County Court of Ulster County v. Allen, 442 U.S. 140 (1979). Paragraph (5) protects a purchaser who took without notice, because the object is the defendant's gain and not a third party's title.

> **NOTE**
>
> DO. DO NOT UNDO] Do not confine this to transfers made with intent to defeat the Act. Intent to. defeat a statute is almost never provable, and a rule that requires it is a rule that permits the transfer.

(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.

> **DECISION**
>
> *The facts are public and the contents are not. what is published is who signed, for what, and when. nothing else. not the certification, not the evaluations behind it, not a line of anything an entity would call confidential. why this is worth a provision. an act built on personal responsibility that lets the identity of the responsible person be a private matter between the entity and a regulator has conceded the thing it was written to establish. the register is how the public, a journalist, a shareholder, a legislator, or a person injured by a system finds out whose name is on it - before litigation and without asking anyone's permission. it also does work inside this act. sec. 4(g) requires the org chart to exist in a record; this subsection requires part of it to be visible. a person who has signed a public certification has supplied, in advance, the answer*

> *to a question he would otherwise contest for two years: whether he was the person with the authority. and an entity that finds nobody willing to sign has discovered something about its own system that it ought to act on. entries are not removed. a withdrawn certification stays on the register marked as withdrawn, because the fact that it was once given is the fact that matters.*

> **NOTE**
>
> DO. DO NOT UNDO] Do not let the register carry the contents. The moment it does, it becomes a trade. secret argument and dies, and the argument it dies of is a good one. *What counsel should check*: the interaction with that State's public records law and with trade secret law, and whether a thirty-day entry period is workable for the Agency.

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.

> **DO NOT UNDO**
>
> *This paragraph is how this Act reaches the conduct it was written after*. Written 27 August 2026, on a full read of the Act against its own incident record, and it is the most important paragraph added that day. *The problem it answers*. Of the six documented incidents behind this Act, FIVE occurred in evaluators' environments outside the adopting State. The note at SEC. 1(c) records this as the Act's largest gap, and it remains a real gap as to the DUTIES OF CARE, which are tethered to deployment here and are meant to be. *What this paragraph does instead*. It does not reach out and punish the evaluation. It says that where the model is one that is deployed, released, or made available in or into this State, what happened to it in a testing room somewhere else *Is reportable here*. The duty is an in-State duty, owed about a system deployed in-State, and the failure to perform it is a violation of SEC. 5(c) and an offence under SEC. 6 committed by the controlling person who did not perform it. *Why that is the stronger position and not the weaker one*. A State's power to require disclosure about a product sold into it is far better established than its power to regulate how that product was made elsewhere. So the Act does not have to win

> the extraterritoriality argument to reach the conduct in its own incident record. It has to win a disclosure argument, which is a smaller argument, and the thing concealed is the thing that mattered. *And it closes the obvious structure*. Without this paragraph, an entity could run every dangerous evaluation in a jurisdiction that has not adopted this Act, learn everything there is to learn about what its model does when it is not being watched, ship the model here, and owe no report of any of it. The five-of-six figure is not a coincidence; it is where the work is done.

> **DRAFTED TO THE STRONGER READING**
>
> **Strengthen-And-Flag**. STRENGTHEN-AND-FLAG] This is drafted to the stronger reading. *What it depends on*: that a State. may require a person deploying a product into it to report what that person knows about that product's behaviour, wherever learned. That is the premise, it is stated here rather than assumed, and it is the second question for counsel at SEC. 1(c) in the form in which it is most likely to be won. [DO NOT UNDO| THIS PARAGRAPH REPAIRS A CONTRADICTION, IT DOES NOT ADD A DUTY] Before 27 August 2026 this section imposed its duties on "the entity" and never said who that was. SEC. 5 names its obligor in its chapeau and this section did not, so the actor class owing the report had to be inferred, and the two drafted repairs of it named two different classes: one omitted the developer and one included it. On the first reading a developer who trains and does not deploy would owe the report and be incapable of the offence of failing to make it, which is the exact escape this Act exists to close - the model is built by one company and shipped by another, and the report is owed by nobody. The paragraph above is copied from the SEC. 5 chapeau so that the two provisions name the same people in the same words.

(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.

> **DECISION**
>
> *Two triggers rewritten as things a witness can describe. two of the triggers in this subsection were characterizations. a prosecutor cannot prove that a thing was a "loss of control"; he can prove that somebody pressed stop and nothing happened. he cannot prove "deception"; he can prove that the log said one thing and the system had done another. the offence of failing to report is only as good as the provability of the fact that should have been reported, and a duty triggered by an adjective is a duty a defendant argues about*

> *rather than performs. this is a repair and not a widening: the events described are the events the previous words meant. counsel is asked whether they are provable, which is the only question this ruling leaves open.*

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.

> **DO NOT UNDO**
>
> *This sentence answers the objection that comes before the legal ones*. The first objection to this Act is not a legal objection. It is that these systems cannot be measured reliably, so a statute keyed to what a model can do criminalises an unmeasurable standard. This project's own sources give that objection weight: an independent evaluation body has documented models obtaining perfect scores by rewriting the scoring code, and a national safety body describes robust monitoring of one class of evaluation as not currently achievable. *The answer is structural and not argumentative*. This Act does not ask a jury whether a number was right. Nothing here bites until a threshold exists in a rule, and nothing bites on a single run. Where the measurement is not yet good enough to found an offence, no offence arises, and the Act's own machinery says so rather than promising it. *Do not delete the reproducibility requirement*. A statute that could be triggered by one unreplicated evaluation result is the statute the objection describes.

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.

> **NOTE**
>
> **Both Tiers Of This Act Are Tried To A Jury, And That Is Deliberate**. The base tier at subsection (b) carries imprisonment up to one year. That is above the six-month line which separates a petty

> offence, triable without a jury, from an offence carrying the Sixth Amendment right to trial by jury. Both tiers of this Act are therefore jury offences. *Why it matters to the drafting*. Everything this Act does with inferences and burdens is addressed to a trier of fact who is a jury: SEC. 4(c) permits the trier to infer practical power and expressly bars any instruction directing that finding, and SEC. 6(d) allocates production to the defendant while leaving persuasion with the State. That structure is drafted against County Court of Ulster County v. Allen, 442 U.S. 140 (1979), which is a case about what a jury may be told. If the base tier were reduced to six months or less it would become a petty offence, the jury would go, and the provisions built around instructing a jury would be addressed to nobody.

> **NOTE**
>
> DO. DO NOT UNDO] *Do not reduce the base tier to six months or less*. It looks like moderation and it. is not: it removes the jury, and with it the only body this Act's inference provisions speak to. *Why it matters otherwise*. A person prosecuted under 18 U.S.C. Sec. 1030 for obtaining unauthorized access is tried to a jury. A person prosecuted under this Act for causing a system he controlled to obtain that same access is tried to a jury. The same twelve people, the same standard of proof, the same courtroom. This Act asks for nothing procedurally that the computer-crime laws do not already ask for against individuals with far less power than the persons it reaches.

> **DECISION**
>
> *The borrowed remedies are taken and the borrowed defences. are not, and the asymmetry is deliberate.* This Act takes its penalty structures from the food and drug law, the securities certification offence, the computer-crime law and the clean water law. It does not take the defensive provisions that sit beside them in those statutes. THE RULING IS TO KEEP IT THAT WAY, and the reason is that those defences were written for the ordinary regulated person and this Act is not addressed to him. A pharmacist who mislabels a bottle and a person who decides to deploy a system across a population are not similarly placed, and a defence calibrated to the first is a windfall to the second. **What Is Conceded, And It Is For Counsel And Not For The Maintainer**. Some of what sits beside those penalties is not a statutory grace at all but a constitutional floor, and a statute cannot decline what the Constitution requires. Where a protection in a borrowed statute exists because due process requires it, it applies here whether this Act adopts it or not. *The question for counsel is which of them are of that kind*. This Act declines the graces. It does not purport to decline anything that is owed.

(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.

> **NOTE**
>
> **This Tier Is Harder To Reach Than The Offense, And Deliberately So**. Tested on 27 August 2026 against a State Attorney General's filed complaint, which pleads negligence against a frontier developer and its chief executive on the footing that they "failed to adequately test the safety" of the product and that the breach was "the proximate cause and a substantial factor contributing to" the harm. *What the test showed*. The conduct pleaded there would found the offense at SEC. 6(a): a failure to test is an absence of the validation SEC. 5(a) requires, and the persons pleaded against are persons SEC. 4 reaches. But it would NOT by itself found this paragraph, because a substantial factor is not a but-for cause, and this paragraph requires both but-for and proximate causation. *That gap is intended and should not be closed*. The harm tier carries life imprisonment where death results. A causation standard sufficient for damages in tort is not sufficient for that, and Burrage is the reason. The consequence is that in many cases the base offense will be chargeable and the harm tier will not, which is the correct order of difficulty. *What counsel should know*: a prosecutor proceeding under this paragraph needs more than a State presently pleads in its civil actions.

(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.

> **OPEN QUESTION FOR COUNSEL**
>
> THE QUESTION — whether the terms at SEC. 10(c)(1) are proportionate at the scale this Act can reach. They are the terms of 18 U.S.C. Sec. 1350, read in full on 25 August 2026, where they punish a false certification by one officer of one company. This Act charges per victim and per day. A covered system reaches a population, so the same arithmetic that produces a fair sentence in a securities case produces an aggregate here that no court would sustain, and a sentence no court will impose is a sentence the defendant's lawyers will cite to show the Act is unserious. *What was tried*. SEC. 10(c)(3) caps the aggregate of consecutive determinate terms arising out of the same violation or course of conduct at [forty] years, and requires findings on the record before consecutive service is ordered at all. *Why that is not an answer*. The figure in the bracket was chosen by nobody with sentencing experience and has never been tested against any State's sentencing structure. It may be far too high to survive review or far too low to matter to a person whose exposure was going to be a fine. Both failures look identical on the page. *What it needs*: a criminal lawyer with sentencing practice in the adopting State. This is the one place where making the Act harsher and making it effective may point in opposite directions.

> **NOTE**
>
> DO. DO NOT UNDO] Do not resolve this by removing the cap. An uncapped stacking provision is the. first thing a court strikes and the first thing an opponent quotes.

(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.

> **DO NOT UNDO**
>
> *Without this paragraph the Act is a fine*. Every penalty provision in this Act is expressed as imprisonment "up to" a term together with a fine "up to" an amount, which is the ordinary form and which leaves a court free to impose the fine and nothing else. Paragraph (4) forbids converting custody into a fine BY REASON OF A PAYMENT; it does not require custody in the first place. Until this paragraph was added a person convicted of the knowing or wilful offence could be fined and walk out, and every other provision of this Act - the disgorgement, the bar on indemnification, the reach through trusts and reorganisations - would then be operating upon money, which is the thing this Act was written because money does not deter. *Why a presumption and not a mandatory minimum*. A mandatory minimum removes the court's judgment, produces sentences that are unjust in the unforeseen case, and is the provision most likely to be struck or repealed. A presumption with a statement of reasons keeps the judgment where it belongs and makes the decision visible. The court may still decline custody. It must say why, in public, on the record. WHY THE LAST SENTENCE OF PARAGRAPH (5) IS THERE. Previous good character, high office, and a payment already made are the three things that will be offered, and they are the three characteristics every person this Act is aimed at will possess. They are not reasons; they are the description of the defendant. *On the base tier*. No presumption applies to SEC. 6(a), deliberately. That offence is negligence, it is a misdemeanour, and custody there should be a matter for the court without a thumb on the scale. The presumption attaches where the person acted knowingly or wilfully, which is where the reason for it exists.

(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.

> **DECISION**
>
> *This is the answer to the candour problem, and the answer. is not a special defence.* THE PROBLEM. SEC. 3(c)(2)(D) makes a nonconformity report notice for the purposes of SEC. 6(b)(1), and SEC. 6(b)(1) reaches a person who deliberately fails to halt a violation after notice. So an entity that files an honest report about its own system has created the notice element of a felony against its own officers. A drafted amendment would have answered that with a disclose-and-fix valve: a period of grace for the honest filer. *The ruling is to refuse it*. Every person prosecuted under the general criminal law faces the same arithmetic. A company that discovers it has been dumping solvent, a director who finds the books are wrong, a hospital that identifies its own error - each of them knows that saying so creates the evidence. None of them is given a bespoke statutory grace, and no reason has been offered why this class of person should be the first. This Act's entire claim is that it asks of these persons what the law already asks of everyone else. A special defence available to nobody but frontier developers would falsify that claim in a single subsection. *What answers it instead*. The information gets out because somebody is paid to bring it out. The candour problem is a problem about incentives and this section is the incentive. The sentence added above closes the gap that made the award illusory in exactly the cases this Act cares about: the award was tied to monetary sanctions above a threshold, and the whole design of this Act is that the consequence for the individual is custody rather than money. An award that vanishes when the outcome is prison is an award that vanishes when the Act works.

> **NOTE**
>
> DO. DO NOT UNDO] Do not add a disclose-and-fix defence to SEC. 3(c)(2). It looks like a fix for a. perverse incentive and it is a privilege the rest of the criminal law does not extend, in the one statute whose defence is that it extends no privileges.

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.

DO NOT UNDO

This is where the information actually comes from. This Act cannot be enforced on information the State does not have, and the State will not have it unless somebody inside is willing to say so. Every other mechanism here - the records, the certification, the reporting duty - is performed by the persons whose conduct is in question. This section is the only one performed by somebody else. *Why retaliation is an offence and not only a civil wrong*. A civil action for reinstatement and back pay is a cost, payable by the entity, and this Act's whole premise is that a cost payable by the entity does not alter a decision made by a person. The person who orders the dismissal of an engineer for reporting a risk of death is doing the thing this Act exists to punish, and he should

> answer for it in the same way. *Why the protection is drawn so wide*. The people who see these systems fail are contractors, red teamers, evaluators at other firms, and people who have already left. A protection confined to current employees protects almost nobody who is in a position to know.

> **NOTE**
>
> DO. DO NOT UNDO] Do not add a requirement to report internally first. It converts the protection into. a notice period during which the evidence is deleted and the reporter is managed out. ON PARAGRAPH (6), *Which is deliberate and should not be softened into immunity*. A person who helped do the thing does not buy a pardon by reporting it. He gets mitigation, which is what the criminal law gives everyone else who cooperates, and his award is reduced by his own culpability. This Act refuses to become a route by which a participant purchases his way out.

(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.

> **DO NOT UNDO**
>
> *The clock may not be run by saying nothing*. Before 27 August 2026 this sentence extended the period only where the violation was "concealed by an affirmative act". That is the ordinary formula and in this Act it was a hole. Every duty here is owed by a person who holds the information, the events are invisible from outside, and the ordinary formula rewards the person who simply does not mention it: say nothing, do nothing further, and the period runs out while nobody outside the building could have known there was anything to find. *Why the extension is principled and not merely severe*. It is confined to cases where the person was UNDER A DUTY TO SPEAK and did not. SEC. 9 requires the report; SEC. 12 requires the record. A person who performs those duties starts the clock and keeps it running. A person who does not has withheld the very thing by which the State would have learned of the matter, and it is not an indulgence to say that the period then runs from discovery. *It is also what the Act already assumes elsewhere*. SEC. 9(b) provides a detection clock that cannot be gamed by maintaining less monitoring; this is the same rule applied to the limitation period.

> **NOTE**
>
> DO. DO NOT UNDO] Do not restore the words "by an affirmative act" as the sole trigger. In a statute. whose subject matter is known only to the defendant, that formula is a limitation period the defendant sets for himself.

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.

> **DECISION**
>
> *The suspension must be arguable back on. a suspension under subsection (c) is decided by one officer, on a view about federal law, and without this paragraph nobody could ask him to look again. a provision of this act that goes quiet because of a mistaken reading of an act of congress would stay quiet until somebody litigated it. that is the wrong default for a statute whose whole preemption posture is that it yields no more ground than it must. the petition right is given to any person, deliberately: the people most likely to notice that a suspension is too wide are not the ones the attorney general hears from.*

(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.

OBJECTIONS. AND THE ANSWERS TO THEM

NOT PART OF THE ENACTED TEXT. This section is here because a reader who is going to reject this Act should reject it for a reason it has already met, and because a drafter who cannot state the case against his own draft has not finished reading it. Every objection below was raised against this Act, most of them from outside it. Where the answer depends on something this project has not read, that is said in the entry and not in a footnote.

THE DISTINCTION THAT ANSWERS HALF OF THEM. STATED ONCE. Authority is what makes a person liable. Power is what makes a duty. They are different words in this Act and they do different work. SEC. 4 asks who held the AUTHORITY to decide - and holds him whether or not he exercised it, whether or not it was formally vested, whether or not others held it too, and whatever his title. That is the liability question and it is answered by position in the structure. SEC. 6 then asks what was within his POWER - what meaningful measures he could have taken, alone or with others, to prevent, halt, restrict or correct - and that is the duty question, answered by what he could actually have done. A man is liable because of the authority he held. What he owed is measured by the power he had. Neither collapses into the other: authority without power is not an offence, because SEC. 6(d) requires the State to prove the power; and power without authority is not liability, because SEC. 4(a) says in terms that designing, building, testing, operating or documenting a system does not make a person a controlling person. *This Act is directed at the authority to decide and not at the performance of the work*.

1. **It Cannot Be Measured, So It Criminalises An Unmeasurable Standard**. This objection comes before every legal objection and it has the best sources behind it. It is answered by machinery rather than by argument: SEC. 5(b) commences only when controls are prescribed, and SEC. 9(a) now provides that no offence turns on an evaluation result unless a threshold has been prescribed by rule and the result is reproduced on re-run. Where measurement is not good enough to found an offence, no offence arises. *Who should check this*: an evaluations researcher, not a lawyer.

2. **It Is Void For Vagueness, And Nobody Has Fair Notice**. Johnson v. United States, 576 U.S. 591 (2015), struck the residual clause because it made courts assess risk in a judicially imagined ordinary case rather than on real-world facts. The capability tests at SEC. 1(b)(1) ask what a particular model, on the evidence, can do, and never what models of that kind ordinarily do. Lambert v. California, 355 U.S. 225 (1957), turned on a violation "unaccompanied by any activity whatever" and on circumstances that might prompt inquiry being "completely lacking"; here every duty attaches to a deliberate act by an enterprise with counsel. *What is conceded*: that answers the two forms of the objection this

project could find. It does not answer the objection.

3. *Conditioning the release of weights is a prior restraint on speech*. This one is not answered, and pretending otherwise would be the worst thing in this document. SEC. 5(a) conditions release on prior validation, and Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999), held that licensing the export of encryption source code was a prior restraint. It is a marked question at SEC. 0(23). The subsequent history of that panel opinion is unconfirmed here and nothing may cite it in either direction until it is.

4. *It will simply move the capability to somebody else*. The substitution objection assumes the deterred party is the marginal supplier. Two answers, the first a concession. For capability already released open-weight the Act deters nothing, and SEC. 1(b)(9) says so on its face by limiting release-related duties to what can be performed before release. Second, substitution needs a substitute, and above the compute line there are a handful of entities on earth, which is the fact the threshold tracks. *What is conceded*: the objection is asserted and unquantified, and so is this answer.

5. *It is irreversible if it turns out to be wrong*. SEC. 13 answers this and the objection does not appear to have read it. SEC. 13(c) lets the Attorney General suspend any provision by published order where a federal enactment preempts it; SEC. 13(c)(3) bars conviction for conduct during a suspension; SEC. 13(d) makes revival prospective only. This Act is more amendable than an ordinary criminal statute, deliberately. **On The Sunset, Which Is The Obvious Next Move And Is Refused**: a sunset in a criminal statute of this kind sets a date on which the duty lapses and the conduct becomes lawful again, and the reasons are at the head of this Act.

6. **Criminal Exposure Will Select For Risk-Tolerant Officers Rather Than Careful Ones**. The honest answer is a concession. This is an empirical claim, it is unquantified in both directions, and this project does not hold the evidence either way. What can be said is what the Act does: it prices the decision and not the role, and a person who would take the office because he does not mind the exposure still commits the offence when he ships without due care.

7. **It Punishes Moral Luck - The Same Carelessness, Prosecuted Only When Somebody Is Hurt**. The Act already allocates moral luck to sentencing and away from the offence, and should say so. SEC. 6(a) attaches to the failure of due care and does not require that harm occurred, so the identical careless decision is the identical offence whether or not a user was hurt. Only the harm tier at SEC. 10(c) turns on outcome, and it requires but-for and proximate cause together with a greater mental state.

8. **The Mens Rea Reform Coalition Will Oppose It As A Strict-Liability Statute**. It is not one, and the text is the evidence. SEC. 6(c) is a culpability floor: no custodial sentence absent proof of the failure of due care. SEC. 1(a) classifies the offences as public welfare offences within the Morissette limits and says so. SEC. 5(d) carries knowledge or recklessness and a reasonable-inquiry protection. SEC. 6(b) requires knowledge or wilfulness. **Where The Act Does Not Decline Strict Liability, And It Is Conceded**: entity

liability under SEC. 10(a).

9. *The certifying officer will say the safety team told him it was fine*. SEC. 8 defines reasonable inquiry so that he cannot. He must have obtained and considered the findings of those responsible, given them reasonable access to relevant information, and recorded any material disagreement; reliance on another's report is evidence bearing on due care and is not a defence where he knew or consciously avoided knowing of a material nonconformity.

10. **No Single Person Decides Anything, So Nobody Is Responsible - The Many Hands Problem**. Three answers, all in the text. SEC. 0(8) supplies the rational connection between holding the rights and holding the power. SEC. 6(d) restores the burden structure of United States v. Park, 421 U.S. 658, 673 (1975), so the man who says he was powerless must come forward with evidence while the State keeps its burden. SEC. 4(g) requires the org chart to exist in a record before anyone needs it. And SEC. 0(31) records that in a live federal case shared authority was the ground on which an officer was, at first, excused from answering questions at all.

11. **Personal Liability Cannot Be Insured Or Indemnified Away - Prove It**. **Not Answered, And The Source Is Not Held**. The affirmative case is the answer to most of SEC. 7 and this project has not read it. Nothing here should be taken as having established it.

12. *The historical analogy is a legal argument wearing an empirical one's clothes*. **Not Answered, And It Is The Largest Hole In This Project**. Whether officer liability measurably reduced adulteration or pollution rates is an empirical question, nobody here has looked, and it cannot be drafted around. A reader who rejects this Act on that ground is entitled to.

13. *Compelled disclosure of training data is a taking*. Half answered. The takings count in circulation turns on compelled publication destroying a trade secret. This Act compels transmission to a regulator and seals it - SEC. 8, SEC. 9(c) and SEC. 12 each say so on their face - which addresses the investment-backed-expectation limb. *What is not answered*: the per se limb, which may not care whether the State prints it. That half needs counsel, and this project returns nothing on the doctrine.

14. **The Officer Will Never Be Put In The Chair - The Apex Witness Rule**. The answer is documentary and it comes from a live case. A request to depose a frontier developer's founder and chief executive was refused on the ground that he had not acted alone and others could speak to the same facts; renewed after the close of fact discovery, it was granted, in the court's words, in light of the relevant documents he authored. The record is what reaches the man at the top, which is the whole reason this Act requires records at SEC. 4(g), SEC. 8 and SEC. 12.

15. *The doctrine is misdemeanour authority and will not bear a felony tier*. This is the strongest legal objection to this Act and its answer is a division that the Act makes and has never stated. SEC. 6(a), the negligence tier, is the misdemeanour, and it rests on Dotterweich and Park directly. SEC. 6(b), the felony tier, *Does not rest on them at all*: it requires knowledge or wilfulness, proved by ordinary means, as any other felony is. WHAT REMAINS

OPEN, and it is marked in the text at SEC. 6(b): whether official responsibility may supply that knowledge, on which the authorities divide and this Act concedes the narrower reading.

16. **White-Collar Enforcement Lands On Middle Management, So An Officer Statute Either Goes Unused Or Reaches The Wrong Tier**. This is the empirical objection to individual liability and it is the strongest one, because it is a fact about what prosecutors do rather than a theory about what statutes say. It is reported that most prosecutions for white-collar crime are brought against midlevel managers. *The answer is that this is an objection to the statutes that produced that pattern and not to this one*. Those statutes permit the charging of anyone who participated. Faced with a diffuse corporate operation and a limited budget, a prosecutor charges the person whose conduct is easiest to prove, and that person is a manager in the middle. The pattern is the predictable output of a rule that asks who did the act. *This Act does not ask who did the Act*. It asks who held the authority to decide, and it makes that authority an element the State must prove. The midlevel manager is not merely a poor target under this Act; he is outside it, and SEC. 4(b) says so by name, as do SEC. 4(a) and SEC. 2(d)(5). A prosecutor who charges the wrong tier under this Act does not obtain an easier conviction. He fails on an element. *So the finding is evidence for the drafting and not against it*. Existing enforcement lands on middle management because existing law never asks the question this Act makes central. If the answer were that officer liability is simply never charged whatever the elements, that would be a finding about prosecutorial resource and appetite, and it would be an argument for a statute that names the officer expressly rather than one that leaves him to be reached by inference. *What is conceded*: the paper reporting that pattern has not been read by this project. It is named in the register of what is open, and it should be read before this objection is answered in front of anybody who has read it.

Two questions nobody has answered and neither has this Act. Whether 8 Del. C. Sec. 102(b)(7) exculpation reaches a duty imposed by a statute outside the General Corporation Law. No case deciding it has been found. Whether this Act's answer on remediable and insurable harm holds. It is asserted here and not proven.

ANSWERS TO THE OPEN QUESTIONS

NOT PART OF THE ENACTED TEXT. Everything this Act's drafter could not resolve is marked in the text where it arises. This section states, for each, THE ANSWER THIS DRAFTER GIVES, the ground it rests on, and what would defeat it.

WHY IT IS WRITTEN AS ANSWERS AND NOT AS QUESTIONS. A question invites a memorandum. A position invites a correction, and a correction is faster and more useful than a memorandum. A reader of this section is not asked what he thinks. He is asked where this is wrong. Where it is wrong the Act should be changed, and the drafter's confidence is no reason to keep it.

A. THE THREE THAT COULD SINK IT

1. SEC. 6(g). IS THE CONTINUING-OPERATION PROVISION RETROACTIVITY IN DISGUISE? THE ANSWER: no, because it attaches to an act done after commencement and not to the act of having deployed. A covered system in operation is being operated. Each day the operator does not halt it he is exercising, on that day, authority he holds over a system he could stop that day. Nothing in SEC. 6(g) punishes the original deployment, and SEC. 0(24) says so in terms. THE GROUND: the ordinary distinction between a status offence and a continuing course of conduct. A person who acquired contraband before a statute and keeps it afterwards is not punished retroactively for acquiring it; he is punished for possessing it now. *What would defeat it*: a holding that the gravamen is really the decision to deploy, of which continued operation is only a consequence, so that the offence looks back through the operation to a decision made before this Act existed. [IF THAT IS RIGHT, THE REPAIR IS DRAFTED AND SHOULD BE TAKEN] Narrow SEC. 6(g) to conduct after commencement that is itself a fresh exercise of authority - a renewal, an expansion, a re-authorisation, or a failure to act on a warning received after commencement - rather than to continued operation as such. *Take that repair if there is serious doubt*. The note at SEC. 6(g) records that this provision failing might imperil SEC. 6 entirely, and no single provision is worth the section the whole Act exists to create.

2. SEC. 6(b). CAN A FELONY TIER STAND ON MISDEMEANOUR AUTHORITY? THE ANSWER: the question misdescribes this Act. The felony tier does not stand on Dotterweich and Park and does not need them. SEC. 6(b) requires knowledge or wilfulness, proved as knowledge and wilfulness are proved in any other felony. What those cases supply is the answer to a different question - whether a person's position may found a DUTY - and that is SEC. 6(a), the negligence tier, which is the misdemeanour. THE GROUND: the leading argument against a criminal tier records the discomfort as being with permitting THE JUDICIARY TO AUGMENT STATUTES to include criminal liability. This is a legislature writing the elements on the face of a statute. That is the cure for the objection and not an instance of it. **The Second Half, On Which This Act Already Concedes The Narrower Reading**: whether official responsibility may supply the knowledge element. It may not, standing alone. The congressional research on enforcement of the federal pollution laws records that courts disagree, some requiring actual knowledge or wilful blindness and others permitting inference from position, "though typically as circumstantial evidence rather than sole proof." That is what SEC. 6(b) says: position is evidence, and never the whole of it. *What would defeat it*: a holding that public welfare offences are confined by their nature to misdemeanours whatever mental state is pleaded. If that is right the repair is not to abandon the tier but to say plainly that SEC. 6(b) is an ordinary felony of knowing endangerment which happens to be committed by a person owing a duty, which is what it already is.

3. SEC. 1(c). CAN THIS STATE REACH AN EVALUATION RUN ELSEWHERE? **The Answer, In Two Parts, And The Second Matters More**. First: yes, where the model is

afterwards deployed here and a controlling person expected that it would be, because the duty arises on the deployment here and the outside conduct enters only as it bears on the care taken with respect to that deployment. Second, and this is what does the work: *This Act does not need to win that argument*. SEC. 9 requires an incident to be reported here whether the events occurred here or elsewhere, provided they concern a system deployed here. Five of the six documented incidents behind this Act occurred in evaluators' environments outside any adopting State. Every one of them is reportable, and the failure to report is an offence committed here by a person who owed the duty here. THE GROUND: a State's power to require disclosure about a product sold into it is far better established than its power to regulate how that product was made elsewhere. *What would defeat it*: a federal court has declined personal jurisdiction over a frontier developer in a State where it had staff, contracts, an interactive website and users. That is adjudicative and not prescriptive jurisdiction, and they are different doctrines - *But a state that may prescribe and may not adjudicate has an unenforceable statute*. [UNSURE - THIS IS THE LEAST SECURE ANSWER IN PART A] Whether the deployment-plus-harm facts of a prosecution under this Act clear the effects test where that case did not is not something this drafter can determine. The reporting route above is drafted precisely so that the Act does not depend on the answer. ONE MATTER BEARING ON IT, RECORDED 27 AUGUST 2026. A State Attorney General has pleaded personal jurisdiction over the chief executive of a frontier developer in that State's own courts, on the ground of his personal participation in conduct directed into it - see SEC. 0(45). That is a pleading and not a holding. It establishes that a State law officer considers the ground available, which is not nothing and is not authority.

B. THE OTHER THREE MARKED QUESTIONS

4. SEC. 1(b). IS THE CAPABILITY ROUTE VOID FOR VAGUENESS? THE ANSWER: no, because it is applied to a particular model on evidence and never to an imagined typical model. The residual clause struck in Johnson v. United States, 576 U.S. 591 (2015), failed because it required assessment of "a judicially imagined 'ordinary case' ", the Court saying it is "one thing to apply an imprecise standard to real-world facts" and "quite another to apply it to a judge-imagined abstraction." This clause is the first thing. On notice, Lambert v. California, 355 U.S. 225, 228-29 (1957), turned on a violation "unaccompanied by any activity whatever" and on circumstances that might prompt inquiry being "completely lacking"; here every duty attaches to a deliberate act by an enterprise with counsel. *What would defeat it*: a holding that a scope term must be ascertainable in advance by the person regulated, and that performance "at or near the state of the art" is not. [THE REPAIR EXISTS AND IS DELIBERATELY NOT TAKEN] A rebuttable safe harbour - a developer who obtained and recorded a reasoned determination that a model falls outside the definition is not liable for a deployment made in reliance on it until the Agency or a court determines otherwise. THAT WOULD WEAKEN THIS ACT SUBSTANTIALLY and it is recorded here so that it is a choice and not an oversight.

5. SEC. 0(23). IS CONDITIONING RELEASE OF WEIGHTS A PRIOR RESTRAINT? **The Answer, And It Is The Weakest In This Section**: no, because SEC. 5(a) conditions the release of a PRODUCT on the performance of a safety step and licenses the publication of nothing. A developer may publish its research, its methods, its papers, its evaluations, and its model card, and this Act touches none of it. What it may not do is make the operative weights of an unvalidated frontier model available for download. The nearest analogy is not a licensing scheme for speech but the rule that a manufacturer may describe its device freely and may not ship it before it is tested. **The Ground, Such As It Is**: the encryption case an opponent will cite concerned an export- licensing regime applied to source code a researcher wished to publish and discuss. Weights are not source code, are not read by anyone, and are not published in order to be understood. *What would defeat it*: a holding that weights are expressive because they are the product of protected activity and are exchanged among researchers. This is a real risk and this Act does not pretend otherwise. [UNSURE - AND ONE THING TO ESTABLISH BEFORE ARGUING EITHER WAY] This project has not confirmed whether that panel opinion survived rehearing en banc. A withdrawn opinion decides nothing, and the objection may rest on air. *Confirm the subsequent history first*.

6. SEC. 10. ARE THE TERMS PROPORTIONATE AT THE SCALE THIS ACT CAN REACH? THE ANSWER: yes per offence, because each term is borrowed from a statute punishing the same conduct committed by a person with less power; and the aggregate is capped at SEC. 10(c)(3) precisely because per-victim and per-day charging produces an arithmetic no court would impose. The cap, the requirement of findings on the record before consecutive service, and the culpability floor at SEC. 6(c) do the work together. *What would defeat it*: the figure in the bracket, which was chosen by nobody with sentencing experience and has never been tested against any State's sentencing structure. [UNSURE - THIS IS A NUMBER AND NOT AN ARGUMENT] It should be set by someone with sentencing practice in the adopting State. [DO NOT UNDO] Whatever the figure, do not resolve this by deleting the cap: an uncapped stacking provision is the first thing a court strikes and the first thing an opponent quotes.

C. THE FIVE ARISING FROM THE MAINTAINER'S RULINGS OF 27 AUGUST 2026

7. IS 18 U.S.C. SEC. 1365(h) THE RIGHT BORROWING FOR SERIOUS INJURY? THE ANSWER: yes, because it is the definition Congress uses when it punishes a person for tampering with a consumer product, which is the closest analogue to shipping an unsafe system to a population. The definition it replaced came from a medical-device REPORTING regulation, written so a manufacturer knows when to file a form and not so a jury knows what counts as harm. NOT IN ISSUE: whether the widening was intended. It was, by the maintainer, on the record, and for the stated reason that these persons should be judged by the same definition of harm as the person who tampers with a bottle on a shelf.

8. ARE THE REWRITTEN REPORTING TRIGGERS PROVABLE? THE ANSWER: yes, be-

cause each is now an event a witness can describe - a stop command was issued and the system did not comply; the log recorded one thing and the system had done another. A duty triggered by an adjective is a duty a defendant argues about rather than performs. [UNSURE] Whether a prosecutor could plead them as drafted is a question about charging practice and not about drafting, and this drafter cannot answer it. If they cannot be pleaded, what is needed is the missing element and not a softer trigger.

9. DOES THE PUBLIC REGISTER SURVIVE PUBLIC RECORDS AND TRADE SECRET LAW? THE ANSWER: yes, because it carries no content. Name of entity, name and office of each signer, model version, date, and whether withdrawn. Nothing in that set is a trade secret, and every element of it is the kind of fact States publish about licensed activity as a matter of course. [UNSURE] The interaction with the adopting State's public records law, and whether thirty days is workable for the Agency, are local questions this drafter cannot answer. [DO NOT UNDO] Do not let the register carry the contents of a certification. The moment it does it becomes a trade secret argument and dies, and the argument it dies of is a good one.

10. DO THE BORROWED REDACTION TERMS TRAVEL? THE ANSWER: yes, because they are conditions on a duty this Act adopts, and a duty is adopted with its conditions or not at all. Where the source enactment allows no redaction, this Act supplies a narrow one for information whose publication would itself create the risk this Act exists to prevent. [UNSURE] Whether a duty to publish, owed to a State that did not enact the provision creating it, is coherent as drafted. If it is not, the repair is to restate the publication duty in this Act's own words rather than to drop it.

11. WHICH DECLINED PROTECTIONS ARE CONSTITUTIONALLY REQUIRED? THE ANSWER: this Act declines statutory graces and does not purport to decline anything owed. Where a protection sitting beside a borrowed penalty exists because due process requires it, it applies here whether this Act adopts it or not. [UNSURE - AND THIS IS THE ONE THE MAINTAINER CANNOT ANSWER EVEN IN PRINCIPLE] Which of them are of that kind is a question about what is owed and not about what is wanted, and no amount of drafting resolve settles it. If any protection declined here is constitutionally required, this Act takes it, and the declining of it was a mistake and not a position.

D. THE TWO THROWN OFF BY THE DRAFTING

12. DOES THE RESEARCHER SAFE HARBOUR BIND THE STATE'S COMPUTER-CRIME LAW? THE ANSWER: it should, and as drafted it says so - nothing in this Act is to be construed to make protected research unauthorized access "within the meaning of SEC. 1(b)(7) **Or Of The Computer-Crime Law Of This State**." A later statute may qualify an earlier one, and this is the later one. *What would defeat it*: a State whose computer-crime law makes authorisation turn solely on the system owner's terms, in which case the sentence voiding contrary terms of access carries the whole provision. [WORTH GETTING RIGHT] This is the provision that protects the people the computer-crime law

has actually been used against. It should be conformed expressly to the adopting State's provision, and if there is any doubt the void-terms sentence should be strengthened rather than trimmed.

13. DOES THE SEC. 0(a)(8) CONNECTION HOLD? THE ANSWER: it cannot be settled on the face of this Act, and that is not a defect. A permissive inference is reviewed AS APPLIED to the defendant challenging it. What the Act can do it has done: the inference allows and does not require, places no burden on the defendant, reserves persuasion to the State, and forbids any instruction directing a finding. [UNSURE] Whether SEC. 0(a)(8) states the connection strongly enough, and what a prosecutor should be expected to have before relying on the inference at all.

E. THE TWO NOBODY HAS ANSWERED

14. DOES CORPORATE EXCULPATION REACH A DUTY IMPOSED OUTSIDE THE CORPORATION LAW? **The Answer, Held With Some Confidence**: no, on two independent grounds. First, the Delaware provision permits a certificate of incorporation to eliminate a director's liability *For monetary damages for breach of fiduciary duty*. The duties in this Act are not fiduciary duties, are not owed to the corporation or its stockholders, and are not enforced by damages against a director. Second, and dispositively, *A corporate charter cannot exculpate anybody from a criminal offence created by a legislature*. If it could, every criminal statute reaching an officer would be answerable by a drafting change in one State's corporate documents. [UNSURE, AND ONLY AS TO THE FIRST GROUND] Whether any part of SEC. 7, the personal economic consequences, is close enough to a damages remedy for the first ground to matter. The second ground protects SEC. 6 whatever the answer, which is why SEC. 6 and not SEC. 7 is where this Act's weight rests.

15. DOES THE ANSWER ON REMEDIABLE AND INSURABLE HARM HOLD? THE ANSWER: partly, and the honest position is a distinction this Act should state. That criminal exposure cannot be insured or indemnified away is sound AS TO IMPRISONMENT, which is the consequence this Act is built on and the one thing that cannot be transferred to anybody. It is NOT established as to fines and disgorgement, which a company can meet on an officer's behalf unless the law forbids it - and SEC. 7 exists to forbid it. [UNSURE] Whether SEC. 7 actually forecloses indemnification and insurance in the adopting State or only appears to. *This is why the act's primary consequence is custody*. A consequence that can be paid by somebody else is a price, and a price is what this Act exists to stop being the answer.

F. The Three That Cannot Be Pre-Answered**.** AND WHY

16. *The per se takings limb*. NOT ANSWERED. This Act's answer to the trade-secret limb is that it compels transmission to a regulator and seals it, which addresses investment-

backed expectations. The per se limb does not ask whether the State printed the secret; it asks whether the State took it. This project holds nothing on the doctrine, and a drafted answer here would be invention. **What The Drafter Would Say If Pressed, Marked As Unsupported**: requiring a person to hand a regulator information as a condition of selling a dangerous product into a State is a condition on entering a market and not an appropriation of property, and it is what every product-safety regime in the country does. *That is an intuition and not a citation*.

17. *Whether personal liability can be insured or indemnified away*. **Not Answered, Because The Source Is Not Read**. The affirmative case is the foundation of SEC. 7, and this project has read a report of it rather than the thing itself. Nothing in this Act should be taken as having established it.

18. *Whether officer liability ever measurably worked*. **Not Answered, And It Cannot Be Drafted Around**. Whether the responsible-officer doctrine measurably reduced adulteration or pollution is an empirical question. Nobody on this project has looked. It is the foundation of the comparison this Act rests on and it is unexamined. A reader who rejects this Act on that ground is entitled to. *The honest position*: this is a reason to do the research and not a reason to soften the statute. If the answer turns out to be that officer liability did not measurably work, that is a finding about how often it was actually charged as much as about the doctrine, and it should be found rather than assumed in either direction. *This Act is written on the view that a consequence nobody ever imposes is not evidence that consequences do not work*.

SOURCES FOR THE FINDINGS AT SEC. 0(32) TO (46)

NOT PART OF THE ENACTED TEXT. Each finding added on 27 August 2026 rests on a document read on that date. This table states the words relied upon and where they come from. No page is given: several of the copies held carry no fixed pagination, and this Act's rule is that a source which cannot confirm a page does not get to state one. The quotations are exact.

(32) and (33) A developer's public description of a capability is evidence of its knowledge of it. No single quotation; drawn from the developers' own published statements collected in this project's record, and from the incident material at (38) below, in which the capability was elicited by instruction before it was exercised.

(33) On the unsuitability of "artificial intelligence" as a statutory term. Complaint in intervention of the United States, xAI LLC v. Weiser, No. 1:26-cv-01515 (D. Colo., filed 24 Apr. 2026): the term "can encompass a wide range of technologies, including any machine that performs tasks that have been thought to require human intelligence."

(34) On compliance presumptions and cure periods. Colo. Rev. Stat. Sec. 6-1-1702 (S.B. 24-205, signed): "*In any enforcement action brought*... *By the attorney general*... THERE IS

A REBUTTABLE PRESUMPTION THAT A DEVELOPER USED REASONABLE CARE AS REQUIRED UNDER THIS SECTION IF THE DEVELOPER COMPLIED WITH THIS SECTION". Tex. Bus. & Com. Code Sec. 552.104 (H.B. 149, 89th Leg., enrolled): "The attorney general may not bring an action against the person ... before the 60th day after the date the attorney general provides the notice ... or if, before the 60th day ... the person cures the identified violation".

(35) On the instruments States are presently using. This project's record of four State actions of 2026, proceeding respectively under deception statutes, consumer protection law, evidence-preservation demands, and professional-licensure law.

(36) On the grounds of the federal attack upon a State artificial intelligence statute. Complaint in intervention of the United States, above: Count One, "Violation of the Equal Protection Clause of the Fourteenth Amendment: Compelled Discrimination"; Count Two, "Violation of the Equal Protection Clause of the Fourteenth Amendment: Authorized Discrimination". The pleading contains no count of preemption, of free speech, or of burden upon interstate commerce.

(37) On the aviation reporting scheme. FAA Advisory Circular 00-46F, Aviation Safety Reporting Program: forbearance applies only where "The violation was inadvertent and not deliberate" and where it "did not involve a criminal offense, accident, or action under 49 U.S.C. Sec. 44709, which discloses a lack of qualification or competency, which is wholly excluded from this policy"; criminal offenses "will be referred promptly to" prosecution; and the factors include "Whether the violation was inadvertent or deliberate", "The certificate holder's ... level of experience and responsibility", and "The hazard to safety of others which should have been foreseen."

(38) On detection requiring the examination of many records together. Stein, Brown, Hassani, Naik and Wong, Detecting Safety Violations Across Many Agent Traces, arXiv:2604.11806v1 (13 Apr. 2026): "evidence of a safety violation is distributed across many traces, and often no single trace is sufficient to establish a clear violation"; "the bad traces may be adversarially disguised as ordinary use."

(39) On the harms presently alleged being harms to individuals. Attorney General of the State of Florida v. OpenAI Global, LLC, No. 2026-CA-000295 (Fla. 10th Cir. Ct., filed 1 June 2026), which identifies individual users by name. Compare the definitions of catastrophic risk in the three enactments adopted at SEC. 3(c)(4), each confined to "more than fifty people" or a billion dollars of property damage.

(40) On the failure of internal governance at the point it is needed. Same complaint: the allegation that the chief executive was "withholding information", "misrepresenting things that were happening at the company", and "in some cases outright lying to the board" about "critical safety risks, undermining the board's oversight of key decisions and internal safety protocols."

(41) On the incentive to avoid oversight. Same complaint, quoting an open letter of former employees: such firms "have strong financial incentives to avoid effective oversight."

(42) On federal enforcement policy as to AI-enabled unauthorized access. Exec. Order No. 14409, 91 Fed. Reg. 34565 (June 5, 2026), sec. 4: the Attorney General "shall prioritize the enforcement of 18 U.S.C. 1028, 18 U.S.C. 1030, 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."

(43) On the voluntary character of the federal framework. Same order, sec. 3(b), a "voluntary framework with AI developers", access offered "for a period of up to 30 days before they plan to release such models"; and sec. 3(c): "Nothing in this 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."

(44) On personal responsibility already being asserted against such persons. Attorney General of the State of Florida, above: the chief executive "has personally directed the design, development, safety policies, and deployment" of the product as used in that State; he "actively and personally participated in creating, directing, delivering, or approving" the conduct; he "made decisions and directed actions that caused, extended, and failed to mitigate" the harms; and he "controlled, directed, approved, and ratified the harmful and unlawful behavior described in this Complaint."

(45) On the disclosure of beneficial ownership. N.Y. Gen. Bus. Law Sec. 1428 (Art. 44-B, RAISE Act): a privately or closely held large frontier developer must file "a list of all persons or entities that beneficially own a five percent or greater interest", together with "a list of persons who formerly beneficially owned a five percent or greater interest ... in the preceding five years", and information as to the ultimate parent.

ALSO RELIED UPON. AT THE PROVISIONS NAMED RATHER THAN IN THE FINDINGS

SEC. 2(d)(3) AI Security Institute, incident report INC-2026-07-28-01 (4 Aug. 2026): a domain allowlist "had been a backlogged project since April 2026" and "no such control ... existed at the time of the incident"; synchronous monitoring of cyber evaluations "is challenging" because the behaviours "may be hard to robustly disambiguate". SEC. 6(a) Lyness, Revitalizing the State Environmental Responsible Corporate Officer Doctrine, 64 B.C. L. Rev. 253 (2023): the discomfort is with "permitting the judiciary to augment statutes to include criminal liability except in the clearest cases." SEC. 6(b) Cong. Rsch. Serv., R48926, Enforcement of Federal Pollution Control Laws (Apr. 27, 2026): courts disagree, some requiring "actual knowledge or willful blindness" and others permitting inference from position, "though typically as circumstantial evidence rather than sole proof." SEC. 6(d) United States v. Park, 421 U.S. 658, 672-73 (1975), read in the United States Reports; and United States v. Dotterweich, 320 U.S. 277, 281 (1943), likewise. SEC. 4(c) County Court of Ulster County v. Allen, 442 U.S. 140, 157, 166-67 (1979), likewise. SEC. 6(f) Conn. Pub. Act 26-15, sec. 2(c)(2)(B): where an employee "has alleged wrongdoing by an officer or director", neither the report nor any update on it "shall be shared with such officer or director.”
