

119TH CONGRESS
2D SESSION

**DISCUSSION DRAFT — not introduced. Prepared for a sponsor's office and for review by the
Office of the Legislative Counsel.**

A BILL

To establish the AI Security Administration, to require the testing, containment, and incident reporting of frontier artificial intelligence systems, to authorize narrow and judicially supervised emergency restraint, to protect minors and users in crisis who use conversational services, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the "American AI Security Act".

(b) **TABLE OF CONTENTS.**—The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings and purposes.
- Sec. 3. Definitions.

TITLE I—AI SECURITY ADMINISTRATION

- Sec. 101. Establishment.
- Sec. 102. Officers and independent functions.
- Sec. 103. Personnel authorities.
- Sec. 104. Coordination and transfer of functions.
- Sec. 105. Technical Advisory Council.
- Sec. 106. Publication and transparency.
- Sec. 107. Conforming amendments.
- Sec. 108. AI-enabled fraud, impersonation, and synthetic sexual imagery.

TITLE II—FRONTIER ARTIFICIAL INTELLIGENCE SAFETY AND SECURITY

- Sec. 201. Coverage.
- Sec. 202. Tier 2 signals and determinations.
- Sec. 203. Safety case and assessment.
- Sec. 204. Incident reporting.
- Sec. 205. Containment, security, and evidence.
- Sec. 206. Emergency restraint.
- Sec. 207. Accredited assessors.
- Sec. 208. Privacy, purpose limitation, and recipients.
- Sec. 209. Whistleblower protections.
- Sec. 210. Relationship to State law.
- Sec. 211. Frontier developer partnership.

TITLE III—CONVERSATIONAL AND COMPANION SERVICES: MINORS AND USERS IN CRISIS

- Sec. 301. Definitions and scope.
- Sec. 302. Duties to all users.
- Sec. 303. Known or likely minors.
- Sec. 304. Incident reporting.
- Sec. 305. Enforcement.
- Sec. 306. Relation to other law; speech.

TITLE IV—NATIONAL SECURITY AND MILITARY USE

- Sec. 401. Human authority over nuclear employment.
- Sec. 402. Autonomous weapon systems.
- Sec. 403. Artificial intelligence analysis of data on United States persons.
- Sec. 404. National security systems.

TITLE V—PROCUREMENT DUE PROCESS FOR ARTIFICIAL INTELLIGENCE SECURITY ACTIONS

- Sec. 501. Scope.
- Sec. 502. Requirements.
- Sec. 503. Conforming amendments.
- Sec. 504. Review.

TITLE VI—INTERNATIONAL TECHNICAL SUPPORT

- Sec. 601. Role.
- Sec. 602. Functions.
- Sec. 603. Limits and oversight.

TITLE VII—FOREIGN PROVIDERS AND REPRESENTATIVES

- Sec. 701. Nexus and scope.
- Sec. 702. Representative.
- Sec. 703. Domestic intermediaries.
- Sec. 704. Enforcement and limits.
- Sec. 705. Evidence held abroad.

TITLE VIII—RESILIENCE, REMEDIATION, AND REPAIR

- Sec. 801. Program.
- Sec. 802. Eligible activities.
- Sec. 803. Awards and validation.
- Sec. 804. Accountability.
- Sec. 805. Limits.

TITLE IX—ENFORCEMENT, REMEDIES, AND JUDICIAL REVIEW

- Sec. 901. Civil penalties.
- Sec. 902. Enforcement by the Administrator.
- Sec. 903. Review of final actions.
- Sec. 904. Emergency restraint proceedings.
- Sec. 905. Protected information in civil proceedings.
- Sec. 906. Actions to compel discrete duties.
- Sec. 907. Existing rights and safeguards.
- Sec. 908. Studies.

TITLE X—FUNDING, TRANSITION, AND EFFECTIVE DATES

- Sec. 1001. Authorization of appropriations.
- Sec. 1002. Fees.
- Sec. 1003. Transition.
- Sec. 1004. Effective dates and interim reporting.
- Sec. 1005. Continuity during a lapse in appropriations.
- Sec. 1006. Rules of construction.
- Sec. 1007. Severability.

SEC. 2. FINDINGS AND PURPOSES.

(a) FINDINGS.—Congress finds the following:

(1) Artificial intelligence systems are being deployed across the economy and in government at a pace that outstrips the capacity of existing law to test them, to learn of their failures, or to act quickly when a failure threatens life or critical infrastructure.

(2) Documented harms from artificial intelligence already include fraud, impersonation, and the creation of sexually exploitative imagery, including of minors. Failures of containment can occur during training, evaluation, and internal use, not only after public release.

(3) Many popular claims about artificial intelligence risk are overstated or unsupported. Federal law should rest on evidence, state its uncertainty, and distinguish harms that have occurred from harms that are possible.

(4) A voluntary evaluation program cannot compel evidence, enforce containment, receive mandatory incident reports, or give affected persons a protected right to be heard. Those functions require statutory authority, secure capacity, and judicial review.

(5) Several States have enacted laws requiring frontier developers to publish safety frameworks, report critical incidents, or undergo audits. A national standard can reduce conflicting obligations, but only if the Federal protection that replaces a State obligation is actually in force, funded, and staffed.

(6) Regulation cannot guarantee the prevention of every foreign attack or recover model weights that have already been copied. Those limits do not make domestic testing, containment, reporting, and remedies ineffective.

(7) Strategic competition with foreign adversaries is a reason to secure United States artificial intelligence systems, not a reason to exempt them from safety and security duties.

(8) Emergency powers over lawful technology must be narrow, brief, and subject to prompt adversarial review before a neutral court, so that the power to restrain cannot become a power to license by delay.

(b) PURPOSES.—The purposes of this Act are—

(1) to establish an independent Federal agency with the scientific, security, and legal capacity to test frontier artificial intelligence systems and to receive and act on reports of their failures;

(2) to require the developers and operators of the most capable systems to contain them, test them, report serious incidents promptly, and submit a safety case before

irreversible release or deployment of a system confirmed to present a specified high-consequence pathway;

(3) to authorize emergency restraint of a specific system only on evidence of imminent serious harm, for no more than 7 days unless a court, after a meaningful adversarial hearing, continues it;

(4) to protect minors and users in crisis who use conversational and companion services;

(5) to protect privacy, lawful speech, and due process, including in procurement and national security decisions;

(6) to displace State law only to the extent that equivalent Federal protection is in force, funded, and capable; and

(7) to publish what the Federal Government learns, including its own missed deadlines and failures.

SEC. 3. DEFINITIONS.

In this Act:

(1) **ACCREDITED ASSESSOR.**—The term "accredited assessor" means a person accredited under section 207 and assigned by the Administrator to a particular assessment.

(2) **ADMINISTRATION; ADMINISTRATOR.**—The terms "Administration" and "Administrator" mean the AI Security Administration established by section 101 and the Administrator of that Administration, respectively.

(3) **ARTIFICIAL INTELLIGENCE.**—The term "artificial intelligence" has the meaning given the term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

(4) **COMMITTEES OF JURISDICTION.**—The term "committees of jurisdiction" means—

(A) the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Committee on the Judiciary of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Science, Space, and Technology, the Committee on Homeland Security, and the Committee on the Judiciary of the House of Representatives.

(5) COMPELLED RESTRICTION.—

(A) IN GENERAL.—The term "compelled restriction" means any direction, however labeled and whether or not later held lawful, that—

(i) is communicated by or on behalf of the Administrator to a person; and

(ii) purports, under this Act or any other asserted authority of the Administrator, to require the person to stop, suspend, or refrain from, or to materially limit the scope, access, or exposure of—

(I) training, evaluating, operating, deploying, or releasing a covered system or configuration; or

(II) any other specified activity involving a covered system.

(B) SCOPE.—Any order, notice, or direction of the Administrator, including under section 205(f) or 703(b), that requires a person to stop, suspend, materially limit, or refrain from training, operating, deploying, or releasing a covered system or configuration is a compelled restriction and may be imposed only under section 206, except for a condition under section 203(d) on an action described in section 203(a)(1), a notice under section 202(c)(7), or a direction under section 202(b)(7). A duty imposed directly by statute, and an ordinary prospective remedial order that does not require a person to stop, suspend, materially limit, or refrain from such an activity, is not a compelled restriction, subject to section 206(j)(3). Subparagraph (A) shall be applied consistently with this subparagraph. Each exception in this subparagraph is limited to a measure satisfying its own separately enacted actor, predicate, process, and endpoint and remains subject to section 206(j)(3). A label or cross-reference alone does not establish the exception, and a measure that actually continues or evades a section 206 restriction is subject to that section.

(6) CONFIGURATION; COVERED OPERATED CONFIGURATION.—

(A) CONFIGURATION.—The term "configuration" means a specified combination of a model or its weights with the tools, permissions, scaffolding, orchestration, and computing environment through which it operates.

(B) COVERED OPERATED CONFIGURATION.—The term "covered operated configuration" means a configuration of a covered system that is operated, whether in internal use or deployment, with covered access or with access to external systems or persons.

(7) CONGRESSIONAL INTELLIGENCE COMMITTEES.—The term "congressional intelligence committees" has the meaning given the term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

(8) CONTROL.—

(A) IN GENERAL.—The term "control", with respect to training or operation of a system, means the actual power, whether sole, joint, or shared, to direct that training or operation, including an enforceable right to approve it.

(B) AGGREGATION.—Operations are aggregated and counted once where persons jointly control, coordinate, or deliberately divide the relevant training or operation.

(C) INDICATORS.—Holding 50 percent or more of voting securities or of rights to profits, or holding contractual power to direct the work, is a rebuttable indicator of control. None of the following, by itself, establishes control: minority ownership, ordinary investment protections, independent unrelated research, ordinary provision of services, or model lineage.

(D) DESIGNATION.—The Administrator may designate a person as having control on grounds of coordination only on evidence of operational power over the covered activity, or of deliberate functional splitting to evade a duty, by a scoped written designation that the person may contest under section 903.

(E) FOREIGN AFFILIATES.—Aggregation under this paragraph reaches a foreign affiliate under common control if the system is made available to persons in the United States or is trained or operated using facilities in the United States.

(F) NO EXEMPTION.—The absence of a single controlling person does not exempt any activity from this Act.

(9) COVERED ACCESS.—The term "covered access" means configured authority, or access realistically obtainable by a system, that together with a capability materially enables a defined pathway to serious harm. Possession of ordinary software tools is not, by itself, covered access.

(10) COVERED CAPABILITY.—

(A) IN GENERAL.—The term "covered capability" means a capability that, under published and reproducible assessment criteria established by rule under section 201(d), materially enables a specified high-consequence pathway to serious harm involving—

(i) chemical, biological, radiological, or nuclear weapons;

(ii) cyber operations capable of serious harm to critical infrastructure or to a substantial number of persons; or

(iii) evasion, disabling, or resistance of authorized monitoring, containment, or shutdown, or acquisition of unauthorized resources or permissions.

(B) TESTING.—Conduct described in subparagraph (A)(iii) is reportable and testable without realized harm, but is not, by itself, a finding of imminent serious harm. Authorized, bounded elicitation of a behavior during testing is not prohibited because it produces the tested behavior. An actual failure of a boundary or stop mechanism is not exempt because it occurred during a test.

(11) COVERED DEVELOPER.—The term "covered developer" means a person that has control of the training of a covered system.

(12) COVERED SYSTEM.—The term "covered system" means an artificial intelligence model or operated artificial intelligence system, including its tool scaffold, orchestration, fine-tuned versions, and relevant derivatives, that—

(A) meets the compute screen established under section 201(a); or

(B) is designated under section 201(b).

(13) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given the term in section 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)). Incorporation of that definition delegates no power and does not establish that any particular digital service is critical infrastructure.

(14) DAY.—Except as otherwise provided, the term "day" means a calendar day. A period stated in hours runs continuously.

(15) DUTY HOLDER.—

(A) IN GENERAL.—The term "duty holder" means, with respect to a covered system, each of the following to the extent of its control:

(i) A covered developer.

(ii) A deployer, meaning a person that makes a covered system available to others as its own offering, or that configures a covered system with covered access.

(iii) A person directing a material modification.

(iv) An orchestration operator, meaning the person accountable for a covered operated configuration.

(v) An environment controller, meaning a person that controls the computing environment, network access, or permissions of a covered system.

(B) RULES.—Each covered operated configuration shall have an orchestration operator, designated in writing by the covered developer or, if the covered developer does not control the configuration, by the deployer, and identified to the Administrator on request. There may be more than one duty holder. Duties follow actual control, and no contract, outsourcing arrangement, or division of components relieves a person of a duty for a function it controls. A provider of general hosting is not an environment controller unless it exercises control described in subparagraph (A)(v).

(16) INTERNAL USE.—The term "internal use" means training, evaluation, research, or operational activity by or for a covered developer or orchestration operator. Duties apply to internal use in proportion to capability, exposure, and control, and sections 204 and 205 apply to internal use without regard to revenue.

(17) IRREVERSIBLE RELEASE; REVERSIBLE DEPLOYMENT.—

(A) IRREVERSIBLE RELEASE.—The term "irreversible release" means making the weights of a covered system, or a configuration from which those weights can practicably be extracted, available to a person outside the control of the duty holder in a manner under which the duty holder lacks the actual, feasible, and continuing technical ability to prevent further use and further distribution of the weights by that person. Contractual terms alone do not establish that ability. A transfer to a recipient that maintains security for the weights meeting the standards under section 205(c), under enforceable terms that permit the duty holder to terminate access and that prohibit further distribution, is not an irreversible release if the duty holder retains that ability. The number of recipients is relevant evidence but is not by itself determinative. Access through a service that the duty holder can revoke, and from which the weights cannot practicably be extracted, is not an irreversible release, regardless of the number of users.

(B) REVERSIBLE DEPLOYMENT.—The term "reversible deployment" means making a covered system available for use by others in a manner that is not an irreversible release.

(18) MATERIAL MODIFICATION.—The term "material modification" means a reasonably supported change to a relevant capability or access pathway, or to the

effectiveness of a safeguard, that meets objective triggers established by rule. A routine change with no material effect on risk is not a material modification.

(19) **PERSON.**—The term "person" means an individual, partnership, corporation, association, organization, or other entity, domestic or foreign, but does not include the United States or an agency of the United States except where expressly provided.

(20) **PROTECTED MODEL WEIGHTS.**—The term "protected model weights" means the weights of a covered system that have not been made publicly available by, or with the authorization of, the covered developer.

(21) **RESTRICTION START.**—The term "restriction start" means the earlier of—

(A) the time a compelled restriction is first communicated to any officer, employee, or agent of the person to whom it is directed, not including an unsent draft or the receipt of unrelated information; or

(B) the time any compelled restriction on a substantially identical pathway first takes legal or practical effect against that person.

The restriction start governs duration only. Sufficiency of notice and culpability for noncompliance are governed by section 206(b)(7).

(22) **SECTOR RISK MANAGEMENT AGENCY.**—The term "Sector Risk Management Agency" has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(23) **SERIOUS HARM.**—The term "serious harm" means—

(A) death or serious bodily injury to one or more individuals; or

(B) incapacity or destruction of, or serious disruption of or damage to, critical infrastructure.

(24) **SMALL ENTITY.**—The term "small entity" means a small business concern, as defined in section 3 of the Small Business Act (15 U.S.C. 632), and a nonprofit organization or institution of higher education with fewer than 500 employees.

(25) **SPECIAL ADVOCATE.**—The term "special advocate" means an attorney appointed under section 905(d) who is independent of the Administrator, free of conflicts, and appointed to advocate for the interests of a person, without an attorney-client relationship, in a proceeding in which that person or its counsel cannot lawfully review protected information, as defined in section 905(a). Appointment of a special advocate does not dilute the person's own right to contest.

(26) STATE.—The term "State" means each of the several States, the District of Columbia, each commonwealth, territory, or possession of the United States, and each federally recognized Indian Tribe.

(27) SUBSTANTIALLY IDENTICAL PATHWAY.—

(A) IN GENERAL.—The term "substantially identical pathway" means a pathway to serious harm that relies on the same or a materially similar system or configuration, and the same mechanism of harm, as a pathway that is or was the basis of a compelled restriction.

(B) WHAT DOES NOT MAKE A PATHWAY DISTINCT.—A change of label, a change of recipient entity within a group of affiliated entities, or an immaterial change in configuration does not make a pathway distinct.

(C) DISTINCT PATHWAYS.—Distinctness shall rest on a materially distinct, evidenced pathway, including a newly evidenced material change in capability, access, exposure, or safeguards. A relabeling or new description of substantially the same pathway does not suffice. A genuinely distinct acute pathway newly established by lawful evidence may be acted on under its own predicates, whether or not every underlying fact arose after an earlier restriction.

(28) TIER 2 SIGNAL; TIER 2 SYSTEM.—The terms "Tier 2 signal" and "Tier 2 system" have the meanings given those terms in section 202.

(29) VOLUNTARY COOPERATION.—

(A) IN GENERAL.—A communication from the Administrator is voluntary cooperation, and not a compelled restriction, if—

(i) it states in writing that compliance is voluntary;

(ii) no consequence for noncompliance under this Act is stated, threatened, or imposed; and

(iii) the person to whom it is directed has not been told that it is required under this Act or any other authority, and is not otherwise reasonably led to believe so.

(B) RULES.—A voluntary label does not exclude actual compulsion. The absence of a written statement does not, by itself, make a noncoercive communication a compelled restriction. The Administrator bears the burden of showing that a contested communication was voluntary cooperation.

TITLE I—AI SECURITY ADMINISTRATION

SEC. 101. ESTABLISHMENT.

(a) IN GENERAL.—There is established in the executive branch an independent establishment, as defined in section 104 of title 5, United States Code, to be known as the "AI Security Administration".

(b) ADMINISTRATOR.—

(1) IN GENERAL.—There is established the position of Administrator of the AI Security Administration, who shall be the head of the Administration.

(2) APPOINTMENT.—The Administrator shall be appointed by the President, by and with the advice and consent of the Senate, from among individuals with demonstrated expertise in artificial intelligence, computer security, or the evaluation of technological risk.

(3) TERM.—The Administrator shall serve for a term of 5 years and may continue to serve after the expiration of the term until a successor is appointed and qualified, for not more than 1 year.

(4) REMOVAL.—If the President removes the Administrator, the President shall, not later than 30 days after the removal, transmit to the committees of jurisdiction a written statement of the reasons for the removal. This paragraph does not limit the President's power of removal.

(c) PRINCIPAL DEPUTY ADMINISTRATOR.—There is established the position of Principal Deputy Administrator, who shall be appointed by the Administrator. The Principal Deputy Administrator shall be the first assistant to the Administrator for purposes of subchapter III of chapter 33 of title 5, United States Code, and, during the absence or disability of the Administrator or a vacancy in that office, shall perform the functions and duties of the office only to the extent and for the periods lawfully authorized under that subchapter.

(d) CONTINUITY OF AUTHORITY.—

(1) SUCCESSION PLAN.—Not later than 30 days after taking office, the Administrator shall, by written order transmitted to the committees of jurisdiction, designate in advance an order of succession for the exercise of each authority under section 206, consistent with subchapter III of chapter 33 of title 5, United States Code, including its eligibility requirements, restrictions relating to nominations, and time limits.

(2) **PROMPT DESIGNATION.**—Any designation of an acting officer shall be made promptly after a vacancy arises.

(3) **LIMITS.**—No authority under section 206 may be exercised by an official, other than the Administrator, who is not so designated and lawfully serving. A designation or plan under this subsection does not itself create a lawful acting appointment. A vacancy, or a late designation, does not extend any period under section 206 or permit an otherwise unauthorized officer to issue an order.

(e) **PRINCIPAL OFFICE.**—The principal office of the Administration shall be in the District of Columbia metropolitan area. The Administration shall maintain facilities able to receive, store, and process classified information.

(f) **FUNCTIONS.**—The Administration shall, through the authorities provided in this Act and other applicable law—

(1) **TEST.**—evaluate artificial intelligence systems for capabilities and access pathways relevant to serious harm, including covered systems, systems developed or offered by foreign persons, and publicly released systems that the Administration lawfully obtains, and publish the results subject to section 106(d);

(2) **MONITOR.**—receive, investigate, and publish information about incidents, risks, and misuse of artificial intelligence systems affecting persons in the United States, whether the source is within or outside the United States, including under sections 102(b), 106(g), 204, 206(i), and 304;

(3) **PREVENT.**—administer the duties of title II intended to prevent serious harm, including testing, containment, security of model weights, and emergency restraint under section 206; and

(4) **SUPPORT.**—provide technical support to other agencies, including under sections 104, 108, 602, and 801.

This subsection confers no regulatory, enforcement, or restraint authority that is not expressly provided elsewhere in this Act.

SEC. 102. OFFICERS AND INDEPENDENT FUNCTIONS.

(a) **CHIEF PRIVACY AND CIVIL LIBERTIES OFFICER.**—

(1) **ESTABLISHMENT.**—There is in the Administration a Chief Privacy and Civil Liberties Officer, appointed by the Administrator.

(2) DUTIES.—The Officer shall review each rule, demand, linkage authorization, and data-retention practice of the Administration for compliance with section 208 and with applicable privacy law, and shall investigate complaints of misuse.

(3) REPORTS.—The Officer shall report not less than twice each year directly to the committees of jurisdiction and to the Privacy and Civil Liberties Oversight Board, without prior review or clearance by the Administrator, on the matters described in paragraph (2).

(b) OFFICE OF INCIDENT REVIEW.—

(1) ESTABLISHMENT.—There is in the Administration an Office of Incident Review, headed by a Director of Incident Review appointed by the Administrator for a term of 5 years. The Director may be removed only for inefficiency, neglect of duty, or malfeasance in office, and the Administrator shall report the reasons for any removal to the committees of jurisdiction not later than 30 days after the removal.

(2) FUNCTIONS.—The Office shall investigate serious incidents and material containment failures reported under section 204 or otherwise known to the Administration, to determine their causes and to recommend measures to prevent recurrence.

(3) SEPARATION.—The Office shall not participate in enforcement, in the issuance of a compelled restriction, or in any assessment under section 203. Personnel of the Office may not be directed by enforcement personnel with respect to the conduct or findings of an investigation.

(4) ACCESS.—The Office shall have access to all records held by the Administration that are relevant to an investigation, for the purposes of the investigation only, through personnel holding any clearance the records require, and subject to applicable privilege rulings and the handling requirements of section 208. Access to records held by the Administration is not a substitute for acquisition of other records, which the Office may obtain only through the authorities of section 205(d) and (e) and section 208, on their own predicates and safeguards. Neither the Office nor enforcement personnel may select a substitute for requested evidence and certify its own adequacy.

(5) FINDINGS.—The Office shall publish each final report, redacted under section 106, not later than 30 days after its completion, and shall provide the unredacted report to the Inspector General, the Comptroller General, and the committees of jurisdiction. A finding of the Office as to cause does not determine fault, waive liability, or bar any claim of an injured person.

(6) INDEPENDENCE SAFEGUARDS.—

(A) **QUALIFICATIONS.**—The Director shall have demonstrated technical competence in the investigation of failures of complex technical systems.

(B) **CONFLICTS.**—The Director and personnel of the Office are subject to subsection (d) of section 103 and shall recuse themselves from any investigation in which they have a conflict of interest under applicable law.

(C) **NO INTERFERENCE.**—No officer or employee of the Administration may prevent, delay, or condition the initiation, conduct, findings, or publication of an investigation of the Office, except to the extent required to protect classified information or material that may be withheld under section 106(d), and the Director shall report each such exception to the Inspector General and the committees of jurisdiction.

(D) **ACCESS DISPUTES.**—The Inspector General shall decide in writing, not later than 10 days after it is raised, any dispute concerning access by the Office to records of the Administration, and the Administration shall comply with the decision.

(E) **BUDGET.**—The budget request of the Administration shall identify separately the amounts requested for the Office.

(c) **INSPECTOR GENERAL.**—The Administration shall have an Inspector General appointed in accordance with chapter 4 of title 5, United States Code, as amended by section 107.

(d) **RESPONSIBLE OFFICIAL FOR REPORTS OF RISK.**—The Administrator shall designate by name a senior official responsible for compliance with section 206(i), who shall report quarterly to the Inspector General on that compliance.

SEC. 103. PERSONNEL AUTHORITIES.

(a) **DIRECT HIRE.**—The Administrator may appoint, without regard to sections 3309 through 3318 of title 5, United States Code, candidates directly to positions in the competitive service in the Administration for which the Administrator determines there is a severe shortage of candidates or a critical hiring need, after public notice. The merit system principles in section 2301 of title 5, United States Code, and the prohibitions in section 2302 of that title apply to appointments under this subsection.

(b) **CRITICAL TECHNICAL EXPERTS.**—

(1) **AUTHORITY.**—Notwithstanding section 3104 of title 5, United States Code, the provisions of that title governing appointments in the competitive service, chapter 51 of that title, and subchapter III of chapter 53 of that title, the Administrator may appoint not

more than 100 scientific, engineering, and professional personnel and fix their rates of basic pay.

(2) **LIMIT.**—The rate of basic pay for a position under this subsection shall not exceed the rate of basic pay for level I of the Executive Schedule. The aggregate of basic pay and any other payment of compensation to an individual under this subsection in a calendar year, excluding employer contributions for retirement, health, and life insurance benefits, shall not exceed the annual rate of salary of the Vice President under section 104 of title 3, United States Code.

(3) **LAWS PRESERVED.**—This subsection does not waive any law relating to ethics, antidiscrimination, the merit system principles and prohibited personnel practices under sections 2301 and 2302 of title 5, United States Code, security requirements, or the availability of appropriations.

(c) **EXCEPTED SERVICE.**—

(1) **AUTHORITY.**—The Administrator may establish positions in the excepted service for personnel who perform evaluation, security, or incident-response functions, may appoint individuals to those positions without regard to the provisions of title 5, United States Code, governing appointments in the competitive service, and may fix their rates of basic pay without regard to chapter 51 and subchapter III of chapter 53 of that title.

(2) **LIMITS.**—The limits in subsection (b)(2) and the laws preserved in subsection (b)(3) apply to positions under this subsection.

(3) **COMPARABILITY.**—In fixing rates of pay under this subsection, the Administrator shall consider rates paid for comparable positions under section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658) and in the private sector. That section does not itself apply to the Administration.

(d) **CONFLICTS.**—No employee of the Administration may participate in a matter involving a person by whom the employee was employed, for whom the employee served as a contractor, consultant, attorney, or agent, or from whom the employee received compensation, during the 2 years before the employee's appointment, or in a matter in which the employee has a disqualifying financial interest under section 208 of title 18, United States Code. For 2 years after leaving the Administration, a former senior employee (as described in section 207(c)(2) of title 18, United States Code) may not knowingly make, with the intent to influence, any communication to or appearance before the Administration on behalf of a covered developer in connection with a matter in which the former employee participated personally and substantially. This subsection is in addition to, and does not shorten or otherwise limit, any restriction under section 207 of title 18, United States Code.

(e) **SECURITY CLEARANCES.**—The Director of National Intelligence shall give priority to the investigation and adjudication of security clearances for personnel of the Administration and for attorneys designated to the panel of special advocates under section 905(d). Priority under this subsection does not establish eligibility for access to classified information and does not extend any period under this Act.

SEC. 104. COORDINATION AND TRANSFER OF FUNCTIONS.

(a) **LEAD-AGENCY AGREEMENTS.**—Not later than 180 days after the date of enactment of this Act, the Administrator shall enter into, and publish, written agreements with the Director of the National Institute of Standards and Technology, the Director of the Cybersecurity and Infrastructure Security Agency, the Assistant Secretary for Preparedness and Response of the Department of Health and Human Services, the Federal Trade Commission, and each relevant Sector Risk Management Agency. Each agreement shall assign responsibility for intake, referral, and response for each category of report under this Act, and shall establish a procedure to resolve disputes between agencies within 14 days. Until an agreement takes effect, reports are received, routed, and given a reasoned disposition under sections 204(e), 204(i), and 1004(b), and an acute warning shall be acted on promptly under existing authority or authority expressly provided in this Act and shall not be held pending an agreement or the product of an assessor.

(b) **SECTOR JURISDICTION PRESERVED.**—Sector regulators retain their jurisdiction over particular uses of artificial intelligence within their sectors. Nothing in this Act limits any authority of another agency under any other provision of law.

(c) TRANSFER OF EVALUATION FUNCTIONS.—

(1) **PLAN.**—Not later than 180 days after the date of enactment of this Act, the Administrator and the Director of the National Institute of Standards and Technology shall jointly publish a transition plan identifying the functions, personnel, records, contracts, and testing and security capacity of the Center for AI Standards and Innovation of the National Institute of Standards and Technology, or any successor organization, that are to be transferred to the Administration, and the functions that the National Institute of Standards and Technology will retain, including the development of measurement science and voluntary standards.

(2) **TRANSFER.**—The functions identified for transfer shall transfer to the Administration on the dates specified in the plan, which shall be not later than 2 years after the date of enactment of this Act. Personnel transferred under this subsection shall be transferred in accordance with applicable law relating to the transfer of functions.

(3) CONTINUITY.—The plan shall include lawful arrangements for continuity of incident intake and handling during the transfer. Those arrangements are planning and response duties and do not guarantee uninterrupted operation.

(4) TRANSFER TERMS.—Upon each transfer under paragraph (2), the personnel, assets, liabilities, contracts, property, records, and unexpended balances of appropriations, authorizations, allocations, and other funds employed, held, used, arising from, available to, or to be made available in connection with the functions transferred shall be transferred to the Administration, subject to section 1531 of title 31, United States Code. Unexpended balances so transferred shall be used only for the purposes for which they were originally authorized and appropriated. Functions not identified for transfer, including the development of measurement science and voluntary standards, remain with the National Institute of Standards and Technology.

(5) COST REPORTING.—The Administrator shall report the costs of transferred functions separately from the incremental costs of the Administration.

SEC. 105. TECHNICAL ADVISORY COUNCIL.

(a) ESTABLISHMENT.—The Administrator shall establish a Technical Advisory Council of not more than 15 members, appointed by the Administrator for staggered terms of 3 years, including independent assessors, academic researchers, representatives of affected communities and of users, representatives of smaller developers, and representatives of covered developers.

(b) LIMITS.—The Council is advisory and has no vote on any action of the Administration. Each member shall disclose the member's employer, clients during the preceding 2 years, and financial interests relevant to the work of the Council. No member may participate in any matter involving the member's employer, such a client, or a person in which the member has a financial interest, or in any other matter in which the member has a conflict of interest under applicable law. Protected information shall be provided to members only under protections equivalent to those in section 208. Participation in the Council is not endorsement of any action of the Administration. No regulated person or class of persons has a veto over any action of the Administration.

(c) FACA.—Chapter 10 of title 5, United States Code, applies to the Council, except that the Council shall not terminate under section 1013 of that title.

(d) PUBLIC COOPERATION COMMITMENTS.—Not later than 90 days after the date of enactment of this Act, the Administrator shall invite covered developers, including leading frontier developers, to submit voluntary written commitments supporting implementation of this Act. A commitment may specify secure testing access, lawfully shareable threat information,

testing infrastructure, technical assistance, and measurable delivery milestones, together with any reservation or dissent. The Administrator shall publish the invitation, the identity and actual commitment status of each respondent, the unprotected terms of each commitment, and annual progress against its milestones. Participation by an employee, an artificial intelligence system, or an advisory council member shall not be described as endorsement by a developer absent an authorized written statement from that developer. A commitment supplies no appropriations, waives no mandatory duty, confers no priority, rulemaking or enforcement authority, and gives no person a veto. Mandatory duties apply independently of participation, signature, or withdrawal. Cooperation shall comply with section 208, applicable fiscal and procurement law, and conflict safeguards; the Administrator may not accept resources on terms that purchase favorable treatment. Agreements under section 211(c) may implement a commitment under this subsection.

SEC. 106. PUBLICATION AND TRANSPARENCY.

(a) **FINDINGS AND DETERMINATIONS.**—The Administrator shall publish, not later than 30 days after taking any final action under title II, a redacted statement of the action and its basis.

(b) **EMERGENCY RESTRAINT.**—Publication with respect to a compelled restriction is governed by section 206(g).

(c) **MISSED DEADLINES.**—The Administrator shall publish, not later than the 15th day of each month, a list of each deadline imposed on the Administration by this Act that was missed during the preceding month, with the reason. Publication does not cure the missed deadline.

(d) **REDACTIONS.**—

(1) **PERMITTED GROUNDS.**—The Administrator may redact from any publication under this Act only—

(A) classified information;

(B) details of an exploitable vulnerability or attack method that is not yet mitigated;

(C) trade secrets and commercial or financial information that is privileged or confidential within the meaning of section 552(b)(4) of title 5, United States Code; and

(D) personal information the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

(2) DOCUMENTATION AND REVIEW.—Each redaction shall be documented with its ground. The Administrator shall review each redaction not later than 180 days after it is made and every 180 days thereafter, and shall release redacted material when the ground no longer applies. Material withheld under subparagraph (B) or (C) of paragraph (1) shall be released not later than 1 year after the original publication unless the Administrator makes a renewed written finding that the ground continues to apply. Before releasing material withheld under subparagraph (C), the Administrator shall give the submitter not less than 30 days' written notice and an opportunity to object, and, except as provided in the following sentence, shall not release the disputed material while a timely objection is pending review under section 903, which the court shall decide expeditiously. A pending objection does not by itself prohibit publication of segregable information that is not lawfully protected, or a necessary timely warning in a form that protects the disputed material; the court may order protection or a stay. Where safe, the Administrator shall give the submitter notice before publishing such a warning. A renewed finding under this paragraph shall state specific reasons.

(3) NO VETO ON WARNINGS.—An opportunity given to any person to correct a draft publication shall not delay an urgent public warning.

(e) OVERSIGHT ACCESS.—The Inspector General, the Comptroller General, and the committees of jurisdiction shall have secure access to unredacted material, subject to appropriate security procedures.

(f) ANNUAL REPORT.—The Administrator shall submit to Congress and publish an annual report that includes minimized statistics on reports received, dispositions and their timeliness, assessments, conditions, compelled restrictions and their durations, lapses and continuations, judicial outcomes, backlog, privacy and security failures, missed incidents identified after the fact, compliance burden, and validated outcomes, with a statement of uncertainty. Statistics on reportable events shall be stated separately for realized harms, attempts, near misses, containment failures, and misuse under section 204(a)(2)(E) and (G). No rate or exposure-adjusted claim shall be published unless it is supported by denominator evidence stated in the report.

(g) PUBLIC THREAT REGISTER AND EVIDENCE AUDIT.—Not later than 180 days after the date of enactment of this Act, and annually thereafter, the Administrator, in consultation with the Federal Trade Commission, the Attorney General, the Cybersecurity and Infrastructure Security Agency, and relevant sector regulators, shall publish a register of documented harms and evidenced threats from artificial intelligence to persons in the United States, whether arising from domestic or foreign conduct. Each entry shall identify the affected population, observed consequence, causal contribution attributed to artificial intelligence,

source provenance, evidence grade under a published method, uncertainty, incidence and exposure denominators where available, and responsible authority and available remedy. Unknown quantities shall be stated as unknown. The register shall distinguish observed harm, attempted or contained conduct, controlled evaluation results, projections, and unsupported claims. It shall identify material overstatement, understatement, and gaps in prominent public and official factual claims, explain each assessment with supporting sources, and offer a public correction process. This subsection authorizes publication and analysis of evidence, not restriction of lawful speech, a new surveillance power, or an inference that an unmeasured harm does not exist. Publication is subject to subsection (d).

SEC. 107. CONFORMING AMENDMENTS.

(a) EXECUTIVE SCHEDULE.—

(1) LEVEL II.—Section 5313 of title 5, United States Code, is amended by adding at the end the following:

"Administrator, AI Security Administration."

(2) LEVEL III.—Section 5314 of title 5, United States Code, is amended by adding at the end the following:

"Principal Deputy Administrator, AI Security Administration."

(b) INSPECTOR GENERAL.—Section 401 of title 5, United States Code, is amended—

(1) in paragraph (1), by striking "the National Security Agency, or the National Reconnaissance Office" and inserting "the National Security Agency, the National Reconnaissance Office, or the AI Security Administration"; and

(2) in paragraph (3), by striking "or the Director of the National Reconnaissance Office;" and inserting "the Director of the National Reconnaissance Office; or the Administrator of the AI Security Administration;".

SEC. 108. AI-ENABLED FRAUD, IMPERSONATION, AND SYNTHETIC SEXUAL IMAGERY.

(a) COORDINATION, NOT DUPLICATION.—The Federal Trade Commission, the Attorney General, the Federal Communications Commission, and each other agency with authority over fraud, impersonation, or the nonconsensual publication of intimate visual depictions retain that authority. This section gives the Administration technical and coordinating functions only, and confers no enforcement authority.

(b) **ASSIGNMENT OF RESPONSIBILITY.**—The plan under section 908(d) shall assign, among the Federal Trade Commission, the Attorney General, and the Federal Communications Commission, responsibility for intake, referral, and response for information concerning the use of artificial intelligence in—

(1) fraud;

(2) the impersonation of an individual, a business, or a government, including by a synthetic voice or likeness; and

(3) the creation or distribution of nonconsensual intimate visual depictions, including digital forgeries within the meaning of the TAKE IT DOWN Act (Public Law 119–12), or of child sexual abuse material.

(c) **TECHNICAL SUPPORT.**—On request of an agency described in subsection (a), the Administration shall provide technical evaluation, including evaluation of—

(1) the effectiveness of safeguards in artificial intelligence models and services against their use to clone the voice or likeness of a real person without consent, to impersonate, or to generate material described in subsection (b)(3); and

(2) methods of detection, authentication, and content provenance, in coordination with the Director of the National Institute of Standards and Technology, who retains the development of measurement science and voluntary standards under section 104(c).

An evaluation of a particular model or service under this subsection requires the consent of its developer or operator or an authority of the requesting agency. Nothing in this section authorizes the creation, possession, or distribution of child sexual abuse material. Any testing that could involve such material shall be conducted only as permitted by law and in coordination with the Attorney General.

(d) **ANNUAL REPORT.**—The Administrator, jointly with the Federal Trade Commission and the Attorney General, shall publish annually a report on the use of artificial intelligence in the conduct described in subsection (b). The report shall use, in aggregate and deidentified form, complaint data of the Federal Bureau of Investigation and the Commission and reports made under section 2258A of title 18, United States Code. It shall state separately reported complaints, adjudicated cases, and estimates, with their uncertainty, and shall identify gaps in Federal law, with legislative recommendations.

(e) **LIMITS.**—Section 208 applies to information under this section. Nothing in this section authorizes monitoring of conversations or content, or regulation of lawful speech.

TITLE II—FRONTIER ARTIFICIAL INTELLIGENCE SAFETY AND SECURITY

SEC. 201. COVERAGE.

(a) COMPUTE SCREEN.—

(1) INITIAL SCREEN.—A model or operated system meets the compute screen if it was trained using a quantity of computing power greater than 10^{26} integer or floating-point operations.

(2) MEASUREMENT.—Operations attributable to training are counted once under a methodology the Administrator shall publish by rule, aggregated across coordinated training runs, relevant derivatives, and persons under common control. Training compute and inference-time compute shall be measured and reported separately, and an equal count of each shall not be treated as equal risk.

(3) ADJUSTMENT.—The Administrator may raise or lower the threshold in paragraph (1) by rule, on published evidence of the relationship between computing power and covered capabilities. The threshold is a policy screen that triggers coverage and the duties that follow from coverage. Meeting it is not a finding that a system is a Tier 2 system, and not meeting it is not a finding that a system is safe.

(4) NOTIFICATION.—A person that begins a training run it reasonably expects to meet the compute screen shall notify the Administrator not later than 30 days after the run begins, and shall notify the Administrator of its completion not later than 30 days after completion, in the form the Administrator prescribes by rule.

(b) DESIGNATION.—

(1) AUTHORITY.—The Administrator may designate a model or operated system as a covered system, regardless of the computing power used to train it, on a written finding supported by evidence that the system, in a specified configuration, has a covered capability or covered access that presents a high-consequence pathway to serious harm.

(2) CONTENTS.—A designation shall state its precise scope, its reasons, its duration, and the conditions for reassessment, and is subject to review under section 903.

(3) VIEWPOINT.—The lawful viewpoint of a person, or of the lawful outputs of its systems, shall not be a ground for designation.

(4) DIRECTION TO ASSESS.—A direction to assess under section 202(b)(7) is distinct from a condition under section 203(d) and from a compelled restriction under

section 206. The lower threshold for a direction to assess does not authorize a condition or a compelled restriction.

(5) RATIONALE.—For each designation, the Administrator shall publish the causal and access rationale, with its uncertainty, subject to section 106(d).

(c) DERIVATIVES AND ASSEMBLED SYSTEMS.—A derivative, fine-tuned, or assembled system is a covered system if it retains or creates the covered pathway, under the applicable criterion of subsection (a) or (b). Lineage alone is not proof that a system is a Tier 2 system. The failure of the Administrator to assess a system is not evidence that the system is safe.

(d) CAPABILITY RULES.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Administrator shall issue rules, after notice and opportunity for comment under section 553 of title 5, United States Code, establishing—

(A) published and reproducible assessment criteria for each covered capability, with the causal and access rationale and its uncertainty;

(B) the criteria for a Tier 2 signal;

(C) a high-consequence criterion for each pathway described in section 3(10)(A)(i) and (ii);

(D) objective triggers for material modification;

(E) the rules required by section 204(a)(2)(B)(i), section 204(c)(1)(A), and section 204(c)(2), and any rules clarifying section 204(a)(3)(F), which may clarify but not narrow it;

(F) the closed list under section 203(b)(1); and

(G) the standards under section 205(c) and (g), except that the standards under section 205(c) shall be issued not later than 180 days after the date of enactment of this Act.

(2) FAILURE TO ISSUE.—The duty in paragraph (1) is a discrete, nondiscretionary duty enforceable under section 906. A failure to issue a rule does not suspend any duty that this Act imposes directly.

(3) FLOORS.—The rules may not narrow the categories of serious harm in section 3(23), the categories of covered capability in section 3(10), or any duty imposed by this Act.

(4) REVIEW.—The Administrator shall review the rules not less than once every 2 years and shall publish the review.

(e) OPEN RELEASES.—Nothing in this Act creates a registry of persons who download publicly released model weights, or imposes a duty on a person solely because that person downloads or uses publicly released weights of a system that is not a Tier 2 system.

SEC. 202. TIER 2 SIGNALS AND DETERMINATIONS.

(a) TIER 2 SIGNAL.—

(1) DEFINITION.—A "Tier 2 signal" is a credible indication, from an evaluation by a covered developer, a third party, or the Administration, of a covered capability or covered access pathway specified in the rules under section 201(d).

(2) EFFECT.—A Tier 2 signal triggers—

(A) proportionate inquiry and scoped testing by the covered developer;

(B) the containment, security, and reporting duties that otherwise apply under sections 204 and 205; and

(C) notice to the Administrator not later than 72 hours after the covered developer forms a reasonable belief that a Tier 2 signal exists.

(3) SEPARATE NOTICE.—The notice under paragraph (2)(C) is separate from a periodic report under section 204(b)(1)(C) and from a report of a severe ongoing threat. One authorized, minimized submission may satisfy overlapping notices.

(4) LIMITS.—A Tier 2 signal is not a finding that a system is a Tier 2 system and, except as provided in subsection (c), imposes no restriction on deployment.

(b) TIER 2 DETERMINATION.—

(1) DEFINITION.—A "Tier 2 system" is a covered system that the Administrator confirms, by a reasoned determination made independently of the covered developer, to have a covered capability or covered access pathway specified in the rules under section 201(d).

(2) START OF PERIOD.—The period for a determination begins at the earliest of the following, as shown by lawful evidence:

(A) Receipt by the Administration of a report of the Tier 2 signal.

(B) Observation of the Tier 2 signal by the Administration, as shown by lawful evidence, whether or not contemporaneously documented.

(C) Actual knowledge of the Tier 2 signal by a responsible official of the Administration.

(3) RECORDS.—The Administration shall record each date in paragraph (2) promptly. A failure to record a known signal, or to record an observation, does not delay the start of the period. Officials responsible for intake and evaluation have reasonable duties of intake and escalation. Nothing in this section imposes a general duty to monitor the internet.

(4) DEADLINE.—The Administrator shall make the determination not later than 30 days after the period begins. The Administrator may extend the period once, by not more than 30 days, by a written decision stating reasons, issued before the original deadline, with notice to the covered developer, who may contest the extension under section 903.

(5) NO RESTART.—The period is not restarted by the late assignment of an assessor, by a date on which testing begins, by relabeling, or by a later notice.

(6) LAPSE.—If no determination is made within the period, the Tier 2 signal lapses as a basis for a determination. The lapse is not a finding of safety, and the duties in subsection (a)(2)(B) and under other law continue. The lapse ends the pending process and supplies no continuing restraint. Known facts remain available to a separately lawful prospective determination with its own evidence, reasons, notice, and review, but no such determination may revive a lapsed process, erase elapsed time, or impose a compelled restriction on a substantially identical pathway except under section 206.

(7) DIRECTION TO ASSESS.—On a Tier 2 signal, the Administrator may issue a written direction, of not more than 30 days' duration, requiring the covered developer to provide the Administration or an assigned accredited assessor with controlled access for testing the specified pathway. A direction is not a compelled restriction, does not restrict training, operation, or deployment, is enforceable under section 902, and is reviewable under section 903. A direction does not extend the period under paragraph (4). This paragraph authorizes scoped assessment access only; its classification as an assessment does not determine whether an actual communication or measure has exceeded that authority or functionally evaded section 206.

(c) PRE-RELEASE DUTY FOR A DEMONSTRATED HIGH-CONSEQUENCE PATHWAY.—

(1) PREDICATE.—This subsection applies to a configuration of a covered system if—

(A) a rule issued under section 201(d) is in effect that establishes a high-consequence criterion for a pathway described in section 3(10)(A)(i) or (ii); and

(B) an assessment specific to the configuration and the pathway, performed by the covered developer or by an accredited assessor, shows that the configuration meets that criterion, taking account of the capabilities, access, and safeguards relevant to an irreversible release.

(2) WHAT DOES NOT SUFFICE.—None of the following, by itself, satisfies paragraph (1): a Tier 2 signal, the compute screen, a label applied by the developer, a claim by a third party, a screened benchmark result, or the copying of weights. A result obtained on a materially different configuration applies only on a showing of relevance. The deliberate removal of a safeguard relied on in the assessment does not avoid this subsection.

(3) DUTY.—A covered developer shall not make an irreversible release of a configuration to which this subsection applies until the process under section 203 for that pathway ends as provided in paragraph (6).

(4) PREPARATION AND SUBMISSION.—The covered developer shall prepare, notify the Administrator of, and submit the initial material specified by rule for the pathway promptly, under its duties of reasonable inquiry and submission. The Administrator shall provide feasible assistance. A covered developer may challenge under section 903 any prerequisite the Administration has made impossible to meet. The start of review under section 203(c) does not depend on a product of an assigned assessor that the Administration controls.

(5) CLOCK.—

(A) RECORDS.—The Administration shall record separately the date of the assessment result, the notice, receipt of the submission, any notice of incompleteness and the actual cure interval, the start of the period under subsection (b)(2), and each decision, deadline, and condition date.

(B) REVIEW PERIOD.—Review under section 203(c) runs from the first receipt of the specified submission, subject only to section 203(b). It does not wait for acceptance by the Administration, the assignment of an assessor, or a Tier 2 determination.

(C) CONCURRENT DETERMINATION.—A determination under subsection (b) runs within the review period from its own earlier start and is not restarted by the review.

(D) NO ADDITIONAL PERIODS.—No additional period may be appended to the review period. A lapsed Tier 2 signal does not satisfy paragraph (1). Guidance may not extend any period. Delay by the Administration does not create an indefinite prohibition, and a developer's failure to meet a pre-release duty is not clearance.

(6) END OF DUTY.—The duty in paragraph (3) ends at the earliest of—

(A) a lawful favorable disposition of the pathway under section 203;

(B) expiration of the review period under section 203(c) without a valid condition under section 203(d) specific to the pathway; or

(C) a documented, reasonably supported determination by the covered developer that paragraph (1) no longer applies to the actual configuration and pathway, accompanied by prompt notice to the Administrator stating the material reasons and supporting information. The determination takes effect when made and does not require prior concurrence. A determination that does not satisfy this subparagraph does not end the duty. The notice shall identify any then-reasonably-planned irreversible release of the configuration and shall be provided promptly when that plan becomes known. Notice under this paragraph is not an application for permission and does not impose a waiting period or postpone the effect of an otherwise valid determination under this paragraph. A release remains subject to any separately applicable statutory pre-release duty, and to a lawful order under its own predicates and safeguards.

(7) CONTEST AND ENFORCEMENT.—The Administrator may contest a determination under paragraph (6)(C) by a reasoned notice identifying the evidence that paragraph (1) continues to apply and may seek timely judicial relief under paragraph (9). The duty in paragraph (3) depends on the actual predicate in paragraph (1), not on concurrence, a pending agency review, or an unadjudicated objection. A disputed notice is not independently conclusive evidence of that predicate and does not restart any period. In judicial enforcement the Administrator shall establish each applicable predicate and the culpability and materiality required for the relief sought. A materially false determination is subject to section 901 only with its applicable culpability and procedure. Any emergency restraint remains subject to section 206.

(8) CHANGED RELEASES.—A materially safer or different release may be reassessed proportionately. A change of lineage, format, or interface, or a minor edit, does not by itself create coverage or avoid this subsection.

(9) JUDICIAL DETERMINATION.—Once the duty in paragraph (3) is presently asserted against a covered developer, including by a notice under paragraph (7), the

covered developer may bring an action against the Administrator, and the Administrator may bring an action against the covered developer, in the United States District Court for the District of Columbia to determine whether paragraph (1) applies. The court shall decide the action not later than 14 days after it is filed, deciding questions of law independently, on the relevant record or an adequate protected substitute under section 905. No administrative exhaustion is required. The Administrator may not withhold a record necessary to the decision while asserting that its protection is complete. Filing does not stay the duty in paragraph (3) unless the court so orders. This paragraph provides the exclusive route of review for the application of paragraph (1), and does not extend or delay any period under section 206.

(10) REVERSIBLE DEPLOYMENT.—This subsection does not apply to reversible deployment. Reversible deployment remains subject to section 203 for a Tier 2 system, to sections 204 and 205, to sector law, and to section 206.

(d) SCOPE OF SAFETY-CASE DUTY.—The requirement of section 203(a) applies to a Tier 2 system. A case under subsection (c) uses the section 203 process for the specified pathway only, and does not deem the system a Tier 2 system or impose other restrictions on deployment.

(e) OTHER RULES.—A covered developer's own threshold label is relevant but not conclusive. Low training compute does not defeat a substantiated capability or access finding. Meeting the compute screen does not, by itself, establish that a system is a Tier 2 system.

SEC. 203. SAFETY CASE AND ASSESSMENT.

(a) DUTY.—

(1) IN GENERAL.—A covered developer, and any other duty holder that materially modifies the configuration or adds covered access, shall not, with respect to a Tier 2 system, or, for purposes of subparagraph (B) only, with respect to a configuration to which section 202(c) applies (for the specified pathway only)—

(A) make a new deployment of the system, or materially expand the access or exposure of an existing deployment;

(B) make an irreversible release of the system; or

(C) enable a new internal configuration that creates a covered pathway of external exposure,

unless the duty holder has submitted a complete safety case, an accredited assessor assigned under section 207(c) has been given the opportunity to assess it, and

the review under subsection (c) has ended without a valid condition that prevents the action, or with a favorable disposition.

(2) ASSESSOR TIMING.—The review period does not wait for the product of the assigned assessor. If the Administrator has not assigned an assessor within 10 days after receipt of the safety case, the duty holder may proceed under subsection (d)(3) at the end of the review period.

(3) EXISTING DEPLOYMENTS.—In the case of a system lawfully deployed on the date of a Tier 2 determination, the covered developer shall submit a complete safety case not later than 60 days after the determination and may continue that deployment during review. No condition under subsection (d) may require withdrawal of an existing deployment. Withdrawal of an existing deployment may be required only under section 206.

(4) CONTAINED EVALUATION.—Contained evaluation may continue under section 205.

(b) COMPLETENESS.—

(1) CONTENTS.—The Administrator shall establish by rule a closed list of the items a safety case must contain, including the system configuration, evaluations performed and their limits, safeguards and their testing, containment and security measures, incident history, and known gaps.

(2) CERTIFICATION.—An accountable officer of the duty holder shall certify that each item on the closed list is present, on the basis of a reasonable inquiry, with a truthful statement of uncertainty. Liability for a false certification requires that the officer or duty holder knew, or recklessly disregarded, its material falsity. There is no liability for facts that could not reasonably have been known.

(3) COMPLETENESS NOTICE.—Not later than 10 days after receipt of a submission, the Administrator may issue one consolidated notice of incompleteness that identifies, with evidence and reasons, each material item on the closed list that is missing. The duty holder shall have a cure period that, in aggregate, shall not exceed 15 days.

(4) DEEMED COMPLETE.—If no notice of incompleteness is issued within 10 days, the submission is procedurally complete. The Administrator may not later claim an omission it did not identify in a timely notice. Procedural completeness is not a finding of safety and does not cure a false statement or a substantive defect.

(5) NO REPEATED PAUSES.—There shall be no second notice of incompleteness, no renewal of the cure period, and no restart of any period by renaming or reopening the

case. No later proceeding may erase procedural completeness, restart or toll a review, or impose a compelled restriction except under section 206. A prospective remedial proceeding on a specified substantive defect requires its own notice, record, authority, and review.

(c) REVIEW PERIOD.—

(1) IN GENERAL.—The Administrator shall complete review not later than 45 days after receipt of the submission, excluding only the actual cure interval under subsection (b)(3), which ends at the earlier of receipt of the cure response or the end of the 15-day cure allowance.

(2) EXTENSION.—The Administrator may extend the review period once, by not more than 30 days, by a written decision stating reasons, issued before the review deadline.

(3) MAXIMUM.—In no case shall the review period exceed 90 days after receipt of the submission.

(4) TIMESTAMPS.—The Administrator shall communicate each timestamp and the resulting deadline to the duty holder promptly, and the duty holder may contest them under section 903.

(5) DISPOSITION.—The Administrator shall issue a reasoned disposition. The Administrator shall publish each quarter the number of pending reviews and the time each has been pending.

(d) CONDITIONS.—

(1) GROUNDS.—The Administrator may impose a condition on an action described in subsection (a) only on a finding of—

(A) materially inadequate containment, authorization of actions, or security;

(B) an assertion in the safety case that remains materially unsupported after reasonable investigation; or

(C) an evidenced high-consequence capability or access pathway that effective safeguards do not address.

(2) CONTENTS.—Each condition shall be issued after notice and an opportunity to respond, and shall identify the defect and the evidence supporting it, the necessary and proportionate remedy, the less restrictive alternatives considered, its duration (which shall not exceed 1 year without renewal on fresh findings), and the grounds for reconsideration. Each condition is subject to review under section 903. A condition applies only to the identified configuration and predicate, and lapses at the end of its duration unless renewed

before then on fresh findings. A pending renewal does not continue a condition, and no condition or renewal extends, or substitutes for, a restriction under section 206.

(3) **PROCEEDING AFTER REVIEW.**—The duty holder shall notify the Administrator of an intended date for the action, and shall update the notice for material changes. A notice neither shortens nor extends the review period. If no condition meeting paragraphs (1) and (2) and no compelled restriction has been issued by the end of the review period, the duty holder may proceed once its other statutory duties are met. A draft or intended condition is not an order. Proceeding is not approval, confers no safe harbor, and does not limit section 206. No person incurs liability solely because the Administrator was still preparing a condition when the period ended.

(4) **SERIAL CONDITIONS.**—A series of conditions used to continue a restraint that section 206 would not permit is subject to section 206(j)(3).

(e) **MATERIAL MODIFICATIONS.**—A material modification of a Tier 2 system requires a proportionate reassessment of the actual system before the modified configuration is enabled, under the procedures of this section.

(f) **NO SAFE HARBOR.**—Completion of an assessment is not a defense to liability. Genuine compliance and reasonable investigation are relevant but not conclusive evidence.

(g) **GOOD-FAITH SELF-EVALUATION.**—A timely, truthful, good-faith disclosure of the results of a self-evaluation is not, by itself, a violation of this Act or an admission of negligence. The underlying facts remain usable, subject to ordinary lawful protections, for coverage, assessment, conditions, section 206, and lawful adjudication of the underlying conduct. No duty holder may, by claim of confidentiality, bar access by a court, the Inspector General, the Comptroller General, or the committees of jurisdiction, or bar publication under section 106.

SEC. 204. INCIDENT REPORTING.

(a) **DEFINITIONS.**—In this section:

(1) **REPORTING ENTITY.**—The term "reporting entity" means a duty holder with control of the covered system, configuration, or activity involved in a reportable event. More than one person may be a reporting entity for the same event. A contract does not transfer the duty to report. A third party may supplement a report but does not discharge another person's duty.

(2) **REPORTABLE EVENT.**—The term "reportable event" means any of the following, occurring in training, evaluation, testing, internal use, or deployment:

(A) SEVERE ONGOING THREAT.—An ongoing course of events, reasonably believed to be occurring, in which a covered system is being used, or is acting, in a way likely to cause serious harm unless promptly interrupted.

(B) MATERIAL CONTAINMENT FAILURE.—An action by a covered system outside its authorized network, permission, authorization, or stop boundary, whether required by section 205 or maintained by the duty holder, or a failure of a required stop mechanism when invoked, that causes or creates any of the following, as reasonably evidenced:

(i) A meaningful failure, bypass, or loss of a safety or security control relied on for the relevant configuration or activity, being a function listed in paragraph (3)(E), a function specified by rule, or a control relevant to a covered capability pathway, with a reasoned connection to material exposure or to a serious-harm pathway.

(ii) Exposure of a protected-data interest described in subparagraph (D).

(iii) Exposure of external systems or persons, in a way that could contribute to serious harm.

(C) SERIOUS INCIDENT.—Serious harm that a covered system is reasonably believed to have caused or materially contributed to.

(D) MATERIAL EXPOSURE OF PROTECTED DATA.—Unauthorized access to, or disclosure of, protected model weights of a covered system, security-relevant configurations of a covered system, or personal data processed by a covered system, that is material under criteria in paragraph (3). A connection to a covered system does not, by itself, make an exposure material.

(E) STATE-ACTOR MISUSE.—Credible evidence that an actor directed by a foreign government has used, or attempted to use, a covered system to plan or carry out an operation that could cause serious harm.

(F) NEAR MISS OR NEW MATERIAL CAPABILITY OBSERVATION.—A detected event that would reasonably have become an event described in subparagraphs (A) through (D) but for intervention or chance, or a new material capability observation meeting the criteria in paragraph (3)(F).

(G) OTHER FOREIGN-STATE MISUSE.—Credible evidence that an actor directed by a foreign government has used, or attempted to use, a covered system, or any other artificial intelligence model or service that a covered developer makes available to others, to plan or carry out—

(i) unauthorized access to a computer system located in the United States or used by a United States person;

(ii) acquisition of protected model weights of any covered developer, or of information about the security of those weights;

(iii) a fraud or impersonation scheme directed at persons in the United States; or

(iv) a covert influence operation directed at persons in the United States, meaning an operation that conceals or misrepresents the role of the foreign government in content intended to influence public opinion or a governmental or electoral decision in the United States.

For purposes of this subparagraph, the covered developer that makes the model or service available is a reporting entity. This subparagraph applies to evidence that the reporting entity has obtained, or that is reasonably discoverable through its existing abuse-detection, security, and enforcement processes. It creates no duty to monitor users or conversations beyond those processes. A report under this subparagraph shall not identify a United States person except as necessary to describe a victim of conduct described in clause (i) or (iii), and shall not describe the lawful speech of any person other than the actor directed by a foreign government.

(3) INITIAL STATUTORY CRITERIA.—Until rules issued under section 201(d)(1)(E) take effect, and as a floor that those rules may clarify but not narrow—

(A) a failure under paragraph (2)(B)(i) of a control relevant to a covered capability pathway is material if it disables, bypasses, or defeats a control that the reporting entity relies on in its safety case, its framework under section 205(h), or its containment plan under section 205 for a covered capability pathway;

(B) an exposure under paragraph (2)(D) is material if it involves—

(i) the unauthorized acquisition of protected model weights of a covered system, by a person outside the reporting entity's control, with a material risk connection to a covered capability pathway;

(ii) the unauthorized acquisition of a security-relevant configuration of a covered system the disclosure of which would materially assist the circumvention of a control described in subparagraph (E); or

(iii) the unauthorized disclosure of personal data processed by a covered system, where the sensitivity, scale, and pathway to exploitation or loss of control of the data present a material risk of serious harm, except that a disclosure of the personal data of 500 or more individuals is rebuttably presumed to be material, a disclosure concerning fewer individuals may be material if the data are highly sensitive, and this clause does not displace any other category under paragraph (2) or any data-breach law;

(C) a near miss under paragraph (2)(F) is any event that would have been an event under any of subparagraphs (A) through (D) of paragraph (2) but for intervention or chance;

(D) each of the following is a red flag for purposes of subsection (c)(1)(A): an unexplained attempt by a covered system to transmit data outside its authorized boundary; an attempt by a covered system to escalate its own permissions or to acquire credentials; a failure or circumvention of a stop mechanism; an unexplained modification of monitoring, logging, or evaluation records; and an unexplained material change in the results of a capability evaluation between comparable runs;

(E) each of the following is a safety or security function for purposes of paragraph (2)(B)(i): a stop or shutdown mechanism; a network or permission boundary; an action-authorization control; a monitoring or logging control relied on for containment; and an access control protecting model weights; and

(F) a new material capability observation is an observation of a reasonably evidenced capability or access pathway of a covered system, identified in its actual configuration, permissions, and safeguards, that is materially different from those previously known to the reporting entity and relevant to a specified serious harm, and the report shall record the evidence, limitations, and uncertainty of the observation. Guidance may explain, but may not create, a duty under this subparagraph.

(4) NOT REPORTABLE.—A failed experiment, a harmless anomaly, or a nominal stop failure is not, by itself, a reportable event. A denied action, or a contained diagnostic anomaly, is not material solely because a log records an external contact. The categories in paragraph (2) do not extend to every untested control, every anomaly, every near miss other than a near miss described in paragraph (3)(C), or every model. An attempt or a containment failure need not result in injury to be reportable if the category is otherwise met. Neither testing status nor the later effective dates in section 1004 exclude an event from a duty that is otherwise in effect. A successful defended test is not a failure under paragraph (2)(B)(i). A test setting is neither an automatic exemption nor evidence of the

frequency of an event in deployment. A numerical presumption in paragraph (3) is rebuttable and does not displace any other category.

(5) REASONABLE-BELIEF ANCHOR.—The term "reasonable-belief anchor" means the earliest legally provable time at which the reporting entity knew, or at which facts reasonably discoverable through the inquiry required by subsection (c) supported, a reasonable belief that an event is within a category of paragraph (2). The anchor is set by provable knowledge or by organizational receipt, and never solely by the date a log entry was made.

(b) DUTY TO REPORT.—

(1) PERIODS.—Each reporting entity shall report each reportable event to the receiver designated under subsection (e) not later than—

(A) 24 hours after the reasonable-belief anchor, for a severe ongoing threat, including a material containment failure that is also a severe ongoing threat;

(B) 72 hours after the reasonable-belief anchor, for a material containment failure, a serious incident, a material exposure of protected data, or state-actor misuse; and

(C) 30 days after the end of each calendar quarter, for near misses, new material capability observations, and events described in subsection (a)(2)(G) during that quarter.

(2) SHORTEST PERIOD.—If an event is within more than one category, the shortest period applies. If an event later worsens so that it first meets the category in paragraph (2)(A) of subsection (a), a new 24-hour period begins, without delaying any earlier report.

(3) NOTHING POSTPONES THE INITIAL REPORT.—The initial report shall not await completion of an inquiry, a final assessment, internal authorization, the availability of an assessor, triage by the receiver, certainty as to causation or attribution, or a confirmed amount of loss.

(4) PROTECTIVE ESCALATION.—A reporting entity aware of a severe ongoing threat shall promptly take feasible lawful steps within its control to interrupt or mitigate it. A reporting period is a maximum, not permission to wait. Where other law or a specific warning duty requires an earlier warning, that duty controls.

(5) UPDATES AND FINAL REPORT.—

(A) UPDATES.—While an event is ongoing, the reporting entity shall update its report upon learning of a material change and not less than once every 72 hours. A

shorter duty under paragraph (1)(A) is not displaced.

(B) FINAL REPORT.—The reporting entity shall submit a final report not later than 30 days after the event ends. An event ends when the reporting entity makes a documented, reasonably supported determination that it is contained and no longer ongoing, unless, not later than 10 days after notice of that determination, the Administrator determines by order that the event has not ended. The order shall state the current facts showing that the event continues and the reasoned scope of the continuing duty to update, and an order that does not state them has no effect. The order is reviewable under section 903. A knowingly or recklessly false determination that an event has ended is a violation of subsection (j)(1)(B); an honest, reasonable determination is not.

(C) EXTENSION.—The Administrator may extend the deadline for a final report once, by not more than 30 days, by a reasoned written decision issued before the original deadline. A pending request does not extend the deadline.

(D) CORRECTIONS.—The reporting entity shall correct any material inaccuracy promptly. A correction shall never delay an urgent initial warning. A final report does not establish safety or end any continuing duty.

(6) SAME PERIODS ELSEWHERE.—The periods in this subsection apply to the corresponding duties under section 304, for the same categories and actors, subject to their separately specified scope. This subsection does not displace an earlier applicable warning or a separately applicable reporting duty, extend a restriction under section 206, or alter another law by implication.

(c) REASONABLE INQUIRY.—

(1) DUTY.—A reporting entity shall carry out a reasonable inquiry, which is an inquiry carried out with the diligence that a prudent duty holder with the entity's control, access, and expertise would exercise in the circumstances, and which includes the minimum inquiry under paragraph (2). In carrying out the inquiry the entity shall—

(A) investigate each red flag listed in subsection (a)(3)(D) or defined by rule that is reasonably within its control;

(B) preserve relevant evidence; and

(C) record the scope, steps, uncertainty, and material limits of its inquiry.

(2) MINIMUM INQUIRY.—The Administrator shall set by rule, for each category, a minimum inquiry covering the relevant configuration, permissions, boundaries, egress

records, and related runs, limited to records that are relevant, technically available, necessary, proportionate, and lawfully obtainable. The minimum is a floor and not a cap, and defined material red flags require escalation beyond it.

(3) LIMITS.—This subsection imposes no general duty to monitor public internet activity, ordinary users, persons who download models, or unrelated persons, and never authorizes a bulk scan of conversations. An incomplete inquiry does not excuse deliberate avoidance of facts that are known or reasonably discoverable. A compliance certificate does not conclusively establish safety.

(d) CONTENTS.—

(1) INITIAL REPORT.—An initial report shall distinguish observed consequences, attempted or contained conduct, material containment failure, and uncertain potential harm, and shall provide the lawfully available information needed to identify the responsible actor, the affected configuration and activity, the category, the observed or reasonably believed pathway, the time of discovery, affected persons or services so far as known, ongoing exposure, containment actions, safe alternatives, and the relevant preserved records.

(2) FACT AND UNCERTAINTY.—Each report shall distinguish observed facts, supported tentative inference, allegation, and unknowns, and shall state the provenance, degree, and basis of any uncertainty about attribution. Unknown quantities shall be reported as unknown. Unsupported attribution shall not be presented as established fact. A need for conclusive attribution to a foreign state does not postpone a report required under any other category.

(3) MINIMIZATION.—Reports shall not include speculative attribution, identifiable private conversation content except as permitted under section 208(c), or unrelated data. The duty to preserve and supply evidence is separate from public disclosure, general access to content, compelled production of model weights, and any duty to notify affected persons under other law.

(4) NO NEW POWERS.—Neither the reporting of state-actor misuse nor its routing creates bulk surveillance, intelligence authority, or a general monitoring duty.

(e) RECEIPT AND ROUTING.—

(1) RECEIVER.—Reports shall be submitted to the Administration or, whenever the Administration's intake is not operative, to the continuity receiver designated in section 1004(b)(2).

(2) RECEIPT.—The receiver shall record actual receipt and provide a protected acknowledgment. Triage follows receipt and does not redefine receipt or postpone any period.

(3) ROUTING.—The receiver shall route each report, in minimized form and only as the report requires, to the following recipients, each of which shall receive only the material necessary for its lawful task, subject to the purpose, use, and retention limits of section 208 and secure handling. A referral does not confer on a recipient the powers of the referring agency. The recipients are—

(A) the Cybersecurity and Infrastructure Security Agency, for a report involving cyber operations or critical infrastructure;

(B) the Assistant Secretary for Preparedness and Response of the Department of Health and Human Services, for a report involving a biological pathway;

(C) the relevant Sector Risk Management Agency;

(D) a protected military channel designated under section 404, for a report involving a national security system;

(E) the Attorney General, where a crime is reasonably indicated;

(F) the Federal Trade Commission, for a report under section 304; and

(G) the Attorney General, for a report under subsection (a)(2)(E) or (G), and the Federal Trade Commission, for a report under subsection (a)(2)(G)(iii).

(4) COMMON SUBMISSION.—A compatible common submission may satisfy overlapping duties only to the extent each applicable law permits, and shall be made by the earliest applicable deadline. This paragraph does not lengthen or postpone any deadline, alter a recipient or substantive predicate required by another law, or excuse an incompatible independently required submission. Additional transmission shall be minimized where lawful and secure. Acknowledgment or routing confers no immunity or clearance.

(5) STATE AUTHORITIES.—The Administrator may share a report, in minimized form, with a State authority that receives incident reports under State law, under a written agreement that protects the report at least as strictly as this Act, under which a State may, at its option and under its own law, treat the Federal report as satisfying its own requirement. Such treatment is voluntary, and is neither an endorsement of the report nor a finding that State remedies are adequate.

(6) ONWARD USE.—Onward use of any report is limited by section 208(e).

(f) CHANNELS AND OUTAGES.—

(1) INTAKE.—The Administrator shall maintain a lawful, secure, and tested intake channel with a safe alternate and actual continuity, applying appropriate safeguards for classified material and for sensitive unclassified material.

(2) NATIONAL SECURITY.—Incidents involving national security systems follow the protected channels designated under section 404. Classification does not exempt an incident from containment or reporting.

(3) DUTY DURING AN OUTAGE.—If the designated channel is unavailable or unsafe, the reporting entity shall use a lawful protected alternate where feasible, document its efforts contemporaneously where feasible, preserve the required evidence, and report within 24 hours after a safe lawful channel becomes available. No reporting entity is required to disclose exploitable details, classified material, or unrelated private content through an unsafe or unauthorized channel.

(4) OUTAGE EXCUSE.—A reporting entity that complies with paragraph (3) is not in violation of subsection (b), as to the information that could not safely be transmitted, for the period during which every genuinely available lawful safe route was unavailable. The unavailability of a preferred channel does not excuse a failure to use an available safe alternate. The entity shall take documented feasible safe alternate steps, including transmitting any required information that can safely be transmitted. An outage does not by itself make a reporting entity strictly liable, and does not waive liability generally, authorize unsafe disclosure, add time under section 206, or suspend any other duty.

(5) FALSE SAFETY CLAIMS.—A claim that a channel was unsafe shall state particularized reasons recorded at the time where feasible, and is subject to secure review. A reporting entity that knowingly or recklessly makes a materially false claim under this subsection is liable under section 901. An honest, reasonable mistake is not a violation.

(g) RECORDS.—Each reporting entity shall keep records of reportable events that are protected and tamper-evident, with verification of integrity and access, gap detection, preservation of known gaps, and a tested response to failures, and shall retain them for not less than 5 years, or for a different period prescribed by rule for a category of record with a stated justification, and for any longer period required by a lawful hold. These duties do not guarantee that every gap will be detected. Retention by the Administration is governed by section 208.

(h) PROTECTION FOR REQUIRED REPORTING.—

(1) WHAT IS PROTECTED.—The act of making a report required by this section, and the disclosures it requires through the statutory channel, are protected. No adverse

inference may be drawn solely from truthful, good-faith reporting.

(2) **WHAT IS NOT PROTECTED.**—The protection does not extend to underlying harmful conduct, to a materially misleading statement, to culpable failure to report or delay, to breach of the inquiry duty, or to unauthorized bulk acquisition or disclosure. Protection is lost under this paragraph only where the applicable wrongful conduct, culpability, and process are established. Honest and reasonable preliminary errors retain protection.

(3) **ENFORCEMENT AGAINST UNDERLYING CONDUCT.**—An enforcement action against underlying conduct requires a particularized lawful basis distinct from the act of reporting, which may rest on lawfully usable facts disclosed in the report. There is no derivative-use immunity and no exclusionary rule, and ordinary privileges and process are preserved.

(4) **WHISTLEBLOWERS.**—Section 209 applies to disclosures under this section.

(i) **DISPOSITION BY THE ADMINISTRATION.**—

(1) **IN GENERAL.**—Each report under this section that is relevant to a risk of serious harm is a report of risk under section 206(i) and shall be preserved, triaged by risk, acted on immediately if it concerns an ongoing acute threat, and given a reasoned, attributable disposition within the period in section 206(i), measured from actual receipt. The disposition period is a process duty; it does not compel any enforcement outcome and is not a reason to delay acting on an acute threat.

(2) **NO TOKEN DISPOSITION.**—A referral or further inquiry shall be meaningful and supported by reasons. Issuing a ticket is not compliance. Consolidation of duplicate reports shall preserve distinct pathways, the chronology, and any gaps.

(3) **TIMELINESS DATA.**—The Administrator shall publish minimized aggregate data on the timeliness of dispositions and shall provide for independent review of follow-through by the Office of Incident Review.

(4) **PROCESS SUIT.**—Under the discrete-duty route in section 906, a court may compel the required disposition process, not a desired discretionary safety outcome. This paragraph does not foreclose any independently authorized substantive remedy on its own lawful predicates, standing, burdens, and process, and does not bar an immediate challenge under section 206.

(5) **LIMITS ON INFERENCE.**—Action or inaction by the Administration on a report does not, by itself, establish causation or liability, or show that remedies available to injured persons are adequate.

(j) VIOLATIONS.—

(1) CONDUCT.—It is a violation of this Act for a reporting entity—

(A) to fail to report, or unreasonably to delay reporting, a reportable event that it knew or reasonably should have known of;

(B) knowingly or recklessly to make a materially false statement or material omission in a report;

(C) knowingly or recklessly to obstruct the inquiry under subsection (c), or to fail to preserve records required by subsection (g), where the obstruction or failure is material; or

(D) recklessly to fail to carry out the inquiry required by subsection (c).

(2) LIMITS.—There is no liability under this subsection for facts that could not reasonably have been known. Honest uncertainty is not a violation. Deliberate ignorance is not a defense. An honest dispute over privilege, an impossible demand, or an accidental gap is not, by itself, obstruction. Truthful uncertainty and a reasonable inquiry are relevant, but are not a conclusive defense to wrongful conduct proved separately. An incomplete report is not, by itself, a violation.

(3) MATERIALITY.—For purposes of this subsection, a statement, omission, delay, obstruction, or failure is material if it has a natural tendency to influence, or is capable of influencing, the receiver's assessment of the category, severity, or pathway of the event or of the response it requires.

(4) PENALTIES.—Violations are subject to civil penalties under section 901. This section creates no new criminal offense and does not repeal or limit any existing law.

(k) EXISTING LAW.—This section does not affect any reporting duty under other law, including under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (6 U.S.C. 681 et seq.) and rules issued under it, section 2258A of title 18, United States Code, or the securities laws. Each such duty keeps its own recipients, predicates, and deadlines.

SEC. 205. CONTAINMENT, SECURITY, AND EVIDENCE.

(a) SAFEGUARDS.—Each duty holder shall maintain, in proportion to the pathway and to its control, and during training, evaluation, internal use, and deployment—

(1) tested network and permission boundaries;

(2) least-privilege identities for systems and agents;

(3) authorization of consequential actions by a mechanism that does not depend on instructions from an untrusted model; and

(4) containment, with tested stop and fallback mechanisms.

(b) **BEFORE ENABLING A HIGHER-RISK CONFIGURATION.**—Before enabling a configuration that materially increases risk, a duty holder shall test the actual system, including against realistic prompt injection and against behavior indicating that the system recognizes it is being evaluated, and shall keep protected, tamper-evident records of the tests. An instruction in a prompt does not, by itself, satisfy subsection (a)(3).

(c) **SECURITY OF WEIGHTS.**—

(1) **IN GENERAL.**—A covered developer shall protect the protected model weights of each covered system against theft and unauthorized access, including by sophisticated actors, foreign state actors, and insiders, under security standards the Administrator shall establish by rule in consultation with the Director of the National Security Agency and the Director of the Cybersecurity and Infrastructure Security Agency.

(2) **LEVELS.**—The standards shall set levels of protection proportionate to the capabilities of the system and the consequences of theft. The highest level shall apply to each Tier 2 system and each configuration to which section 202(c) applies, and shall be designed to resist theft by sophisticated actors, including foreign state actors. The standards for every other covered system shall, at a minimum, provide for the detection of attempted theft and its reporting under section 204.

(3) **BEFORE A DETERMINATION.**—A covered developer shall apply the highest level to a covered system from the time the covered developer forms a reasonable belief that a Tier 2 signal exists until a determination under section 202(b) that the system is not a Tier 2 system, or the lapse of the signal under section 202(b)(6).

(d) **INSPECTION.**—

(1) **IN GENERAL.**—The Administrator may conduct risk-based inspections of the facilities, systems, and records of a duty holder relevant to compliance with this title, including independent tests of boundaries.

(2) **RESIDENT INSPECTORS.**—The Administrator may assign resident inspectors to a covered developer of a Tier 2 system or to a duty holder with persistent failures.

(3) **WEIGHTS.**—The Administrator shall prefer access to weights through controlled means at the duty holder's facility. The Administrator may require transfer of weights only on a particularized written finding that transfer is necessary and proportionate.

(4) NO CENTRAL STORE.—The Administration shall not maintain a central store of models or of conversations.

(5) WARRANT OR CONSENT.—An inspection of a facility, or of records not voluntarily produced, shall be made with the consent of the duty holder or under an administrative inspection warrant issued by a United States magistrate judge or district judge on a showing that the inspection follows a neutral, risk-based inspection plan or that there is specific evidence of a violation. Refusal of an inspection for which no warrant has issued is not a violation of this Act.

(e) EVIDENCE DEMANDS.—

(1) AUTHORITY.—The Administrator may issue a written demand for records, testimony, or access relevant to a duty under this title. Each demand shall specify its scope, necessity, deadline, minimization, and protections. A demand is enforceable only by order of a court under section 902.

(2) EVIDENCE-READINESS PACKAGE.—Each covered developer shall maintain a package containing the relevant configuration and version, permissions, boundaries, stop telemetry, available incident records, retention, and known gaps, consistent with section 204(g) and section 208. Separable material in the package shall be produced not later than 48 hours after a lawful demand, or within any longer period that the demand allows or that is proportionate and reasonably achievable for the material demanded, unless a court orders otherwise. A failure to produce is enforceable under paragraph (1). The package requires no continuous collection of unrelated conversations, no recreation of erased data, and no production of privileged material without lawful process.

(3) DURING A COMPELLED RESTRICTION.—While a compelled restriction is in effect, the Administrator shall seek a particularized, reasonably achievable deadline from the court for any contested production. A challenge does not automatically stay a lawful demand. The court may narrow or stay contested production, protect privileges, and prevent irreparable disclosure. Uncontested separable records and necessary preservation shall proceed promptly. A deliberate breach of a lawful, proportionate, and achievable demand may support separate enforcement and may inform the record, but does not by itself establish imminent harm, shift any burden, or pause any period.

(4) PROTECTIONS PRESERVED.—Lawful protections for trade secrets, privacy, privilege, whistleblowers, and research are preserved. Guidance of the Administrator does not override the law governing communications or intelligence.

(f) ORDINARY REMEDIAL ORDERS.—The Administrator may issue an order requiring a duty holder to remedy a specified violation of this section, after notice, an opportunity to

respond of not less than 10 days, and a written record identifying the statutory defect. An order under this subsection may not require the suspension or cessation of training, operation, or deployment. The order is reviewable under section 903.

(g) **STANDARDS.**—The Administrator shall establish standards under this section by rule after notice and comment. A consensus standard may be incorporated only on a finding that it meets the requirements of this section.

(h) **SAFETY AND SECURITY FRAMEWORK; DEPLOYMENT SUMMARY.**—

(1) **FRAMEWORK.**—Each covered developer shall write, implement, and comply with a safety and security framework that describes—

(A) how it assesses whether a covered system has a covered capability or covered access, including the thresholds it uses and its treatment of internal use;

(B) the safeguards it applies at each threshold, including under subsections (a) through (c);

(C) its use of third-party and accredited assessment;

(D) how it identifies, investigates, and reports events under section 204;

(E) its internal governance, including the officers accountable for the framework and a process by which employees and contractors may report concerns internally, anonymously if they choose; and

(F) how it reviews and updates the framework, which it shall do not less than once every 12 months.

(2) **PUBLICATION.**—The covered developer shall publish the framework, and each material revision not later than 30 days after it is adopted, and shall submit an unredacted copy to the Administrator. The covered developer may redact from the published version only material described in subparagraphs (A) through (D) of section 106(d)(1), and shall identify each redaction and its ground. An unredacted copy containing classified information shall be submitted only through a channel and to personnel authorized to receive it.

(3) **DEPLOYMENT SUMMARY.**—Not later than the date of a new deployment or irreversible release of a covered system, the covered developer shall publish a summary of the capability assessments performed on the system under its framework, their results and limits, the safeguards applied, and the role of any third-party or accredited assessor, subject to the redaction limits in paragraph (2).

(4) STATUS.—A framework is not approved by the Administrator, confers no safe harbor, and does not narrow any duty under this Act.

(5) EFFECTIVE DATE.—This subsection takes effect 180 days after the date of enactment of this Act.

SEC. 206. EMERGENCY RESTRAINT.

(a) AUTHORITY AND STANDARD.—

(1) FINDINGS.—The Administrator may issue a compelled restriction only on a written, particularized determination, supported by lawfully usable evidence, that—

(A) the actual system configuration, access, or activity presents an imminent risk of serious harm;

(B) the risk arises through an evidenced pathway involving that specified configuration;

(C) the restriction is necessary to interrupt or materially reduce that risk; and

(D) no reasonably available, less restrictive control would adequately address the risk, stating the reasons each identified alternative is inadequate.

(2) WHAT DOES NOT SUFFICE.—None of the following, standing alone, satisfies paragraph (1): an indication of a covered capability or covered access, including a Tier 2 signal or a report of risk under subsection (i); a pending assessment or an assessment queue; a delay in, or failure of, reporting under section 204; the irreversible copying of model weights; the capability threshold of any duty holder; a test result, although a controlled test result is evidence that may support a pathway; or a difference from a foreign benchmark.

(3) CONTENTS.—Each compelled restriction shall be in writing and shall state—

(A) the responsible person, identified by control;

(B) the system, configuration, and activity restricted;

(C) the safe functions and configurations that remain permitted, where continuing them is feasible and consistent with paragraph (1);

(D) the restriction start and the time of lapse;

(E) the evidence relied on, its material limits and uncertainty, and a nonclassified summary;

(F) the conditions for narrowing or ending the restriction; and

(G) the assessment required by subsection (h).

(4) PROTECTED NOTICE.—The Administrator shall promptly give the restricted person the factual and legal basis of the restriction through the procedures of subsection (f). A public statement under subsection (g) does not replace that notice.

(5) DECIDING OFFICIAL.—Each compelled restriction shall name the official who made the determination, who shall be the Administrator or an official designated and lawfully serving under section 101(d).

(6) ORAL DIRECTION.—An urgent oral direction is permitted only if the imminence of the risk prevents a written order before communication. The official shall record minimum reasons at the time. The written order shall be served not later than 12 hours after the restriction start, and if it is not, the restriction lapses at that time. Repeated oral notices, or conversion of an oral direction into writing, do not change the restriction start.

(b) DURATION AND LAPSE.—

(1) LAPSE.—A compelled restriction lapses at the earliest of—

(A) 7 days after its restriction start, unless continued under subsection (c) before that time;

(B) the end of the 12-hour period in subsection (a)(6), if that paragraph applies;

(C) the end of the 48-hour period in paragraph (2), if no application has been filed and served within that period; or

(D) the time the court determines that the restriction was not lawfully imposed or is no longer justified.

(2) APPLICATION.—Not later than 48 hours after the restriction start, the Administrator shall file in the court designated under subsection (d), and serve on the restricted person, an application for a determination under paragraph (3). If the Administrator does not do so, the restriction lapses at the end of that 48-hour period.

(3) HEARING AND DECISION.—Before the 7-day period ends, the restricted person shall receive a meaningful, protected, adversarial hearing before the court designated under subsection (d), and the court shall decide whether the requirements of subsection (a)(1) were met at the restriction start and continue to be met. If the hearing and the decision do not both occur within the period, the restriction lapses at the end of the period without further application by any person. An expired restriction provides no

authority for continued compelled restraint.

(4) NO TOLLING.—No event tolls, suspends, or extends any period under this subsection, including service, alternative service, or rules on actual notice; a change of venue, transfer, or appeal; the security clearance of any person; the appointment or availability of a special advocate; the availability of an assessor; the restricted person's compliance or noncompliance; or any request by the Administrator. The powers of the court under subsection (c)(7) do not create an administrative extension.

(5) NO RESET.—A compelled restriction on a substantially identical pathway runs from the earliest restriction start of any prior compelled restriction on that pathway, however the later restriction is framed, including as a new order, a modification, a withdrawal and reissue, a division into parts, a direction to an affiliate, or a move to a nominally different process. A lapsed restriction does not remain in effect while a motion to continue it is pending.

(6) CHRONOLOGY.—The Administrator shall keep a protected, tamper-evident chronology of each restriction start, service, modification, lapse, continuation, and rescission, with integrity and access checks and gap detection, and shall enter each event not later than 24 hours after it occurs. The chronology is evidence; it does not determine legal events, and a delayed or inaccurate entry never postpones a restriction start or cures a lapsed restriction. Access is limited to the court, the restricted person subject to subsection (f), the Inspector General, and the committees of jurisdiction, and the chronology may be used only for the purposes of this section. Known gaps shall be preserved and met with a tested response, and the limits of section 208 on task, recipient, use, retention, and minimization apply. These are duties, not a guarantee that the record cannot be tampered with.

(7) NOTICE AND LIABILITY.—No person may be sanctioned for noncompliance with a compelled restriction unless the restriction was lawful and in effect, the person received legally sufficient notice before the noncompliance, the culpability and materiality required by section 901 are proved, and the applicable procedure is followed. Rules on service or actual notice do not extend any period under this subsection.

(8) PROMPT RESCISSION.—The Administrator shall narrow or end a compelled restriction promptly once its basis under subsection (a)(1) no longer exists for all or part of its scope, including during a judicial continuation, and shall give the court and the restricted person written reasons not later than 24 hours after doing so. The period for giving reasons does not authorize continued restraint.

(c) CONTINUATION BY THE COURT.—

(1) COURT ONLY.—Only the court designated under subsection (d) may continue a compelled restriction beyond the period in subsection (b), on motion of the Administrator.

(2) INCREMENTS.—Each continuation shall be ordered before the prior period ends and shall set a definite expiration not more than 30 days after the order. No administrative period follows a continuation.

(3) FINDINGS.—For each continuation, the court shall find, on currently relevant evidence and after meaningful protected adversarial review under subsection (f)—

(A) a continuing imminent risk of serious harm through the evidenced pathway;

(B) necessity; and

(C) that the continued restriction is the least restrictive adequate measure.

(4) BURDEN AND STANDARD.—The Administrator bears the burden of proof on each finding under paragraph (3), and on each finding under subsection (b)(3), by clear and convincing evidence. The court shall determine those findings independently and without deference to the Administrator's determination. Other questions retain their otherwise applicable standards of review.

(5) ADVERSARIAL FOLLOW-UP.—Each continuation order shall set an enforceable deadline, within the increment, for meaningful adversarial follow-up of defined scope. If the follow-up does not occur by the deadline, the continuation lapses.

(6) NO AUTOMATIC CONTINUATION.—No continuation takes effect by default, by operation of law, or by the passage of time.

(7) COURT POWERS.—The court retains its lawful powers to narrow a restriction, protect information, and stay or vacate a restriction.

(8) BOUNDED JUDICIAL FOLLOW-UP.—A provisional procedure does not authorize restraint beyond the initial period unless, before that period ends, the court has conducted meaningful protected adversarial review and decided each finding required by subsections (b)(3) and (c)(3) under the burden and standard in paragraph (4). After those findings, the court may set a single follow-up period of not more than 72 hours within the judicial increment for identified supplemental matters, only where the current contest is already meaningful and the supplemental procedure does not replace it. The order shall state the scope, reasons, and deadline for both the supplemental hearing and decision. The continuation lapses if either is not completed by that deadline. No prima facie showing, commenced but inadequate hearing, court-only inspection, personnel shortage, or pending request supplies the required initial findings or extends an expired restriction.

(d) CHALLENGE; DESIGNATED COURT.—

(1) IMMEDIATE CHALLENGE.—A person to whom a compelled restriction is directed may seek immediate review in the court designated under paragraph (2). No administrative exhaustion, notice period, bond, or agency scheduling rule bars the challenge. The court shall decide before the restriction or the current continuation lapses. If it does not, the restriction lapses.

(2) DESIGNATED COURT.—The United States District Court for the District of Columbia shall have exclusive jurisdiction of proceedings under this section. The chief judge of that court shall designate not fewer than 3 judges to hear such proceedings and shall maintain an on-call schedule designed to make a designated judge available at all times. If the designated judges are unavailable, any judge of that court may act. Upon presentation of a certificate of necessity by the chief judge or circuit justice of the District of Columbia Circuit, the Chief Justice of the United States may designate and assign additional district judges to that court in accordance with section 292(d) of title 28, United States Code, to meet the demands of this section. No assignment, and no unavailability of a judge, extends any period under this section. The court shall report annually to the committees of jurisdiction any period in which no judge was available to act under this section.

(3) INTERVENTION.—A person whose service to the public, or to critical infrastructure, is materially disrupted by a compelled restriction, and who satisfies the requirements of standing under article III of the Constitution, may intervene as of right under Rule 24(a)(1) of the Federal Rules of Civil Procedure on the question of the scope of the restriction and the adequacy of the safe fallback under subsection (h).

(4) APPEAL.—An appeal lies to the United States Court of Appeals for the District of Columbia Circuit, which shall expedite it to the greatest possible extent. A venue dispute, transfer, or appeal does not extend any period under subsection (b) or (c).

(5) WHETHER A COMMUNICATION COMPELS.—The court shall decide promptly, as a threshold matter, whether a communication is a compelled restriction, and the person challenging may offer evidence of compulsion. The threshold question does not postpone review of the merits or the lapse.

(e) DISTINCT PATHWAYS.—

(1) IDENTICAL PATHWAYS.—A restriction on a substantially identical pathway is governed by subsection (b)(5) and may be continued only under subsection (c).

(2) NEW PATHWAY.—The Administrator may issue a separate compelled restriction for a genuinely distinct, newly evidenced pathway that meets subsection (a) on its own evidence. The restriction shall disclose each relevant prior restriction and state objective reasons why the pathway is distinct.

(3) REVIEW.—The court shall decide distinctness de novo.

(4) LATER PROCEEDINGS.—Lapse of a restriction does not establish safety or confer immunity from a separately lawful prospective proceeding, which may use lawfully usable known facts. No such proceeding may toll, restart, or continue the lapsed restriction on the same pathway, reopen a closed completeness determination, or impose a hold pending review without its own enacted authority and safeguards. A lapsed assessment of an indication described in subsection (a)(2), including a lapsed Tier 2 signal, is not a continuing emergency predicate.

(f) PROTECTED ADVERSARIAL REVIEW.—

(1) SPECIAL ADVOCATES.—The court shall appoint a special advocate under section 905(d) whenever protected information, as defined in section 905(a), is relied on that the restricted person or its counsel cannot lawfully review.

(2) ACCESS.—A special advocate shall have access to the material relied on under section 905. The special advocate may consult the restricted person before reviewing protected information, and afterward subject to protections approved by the court.

(3) SUBSTITUTES.—The court shall require substitute disclosures or summaries under section 905(c) that give the restricted person a meaningful opportunity to respond.

(4) MINIMUM STANDARD.—A purely ex parte proceeding, or inspection by the court alone without participation by a special advocate or counsel, does not satisfy this subsection. Participation of a special advocate is not conclusive proof of a meaningful contest.

(5) NO TIME FOR SCARCITY.—Unavailability of a special advocate, or delay in any clearance, extends no period. If the material relied on cannot be meaningfully contested before lapse, the Administrator may withdraw reliance on it or use a lawful and sufficient protected alternative. Withdrawal or a proposed alternative does not by itself authorize continuation: the remaining lawful record and protected process must support each finding required by subsection (a) or (c), and the hearing and decision must occur within the controlling period, or the restriction lapses. No waiver of competence, unreviewed substitute by the Administration, or additional administrative period is authorized. A special advocate is not required where the restricted person's own counsel

lawfully reviews the evidence and a meaningful contest occurs.

(g) PUBLIC BASIS.—

(1) PUBLICATION.—Not later than 72 hours after the restriction start, the Administrator shall publish a minimized, nonclassified statement of the basis of the restriction, giving the category of harm, the type of pathway, the restricted activity, and the time of lapse. The statement shall not reveal exploitable details and shall not delay an urgent safety warning.

(2) REDACTIONS.—Redactions are limited to the grounds in section 106(d)(1), shall be documented, and are reviewable by the court.

(3) WITHHELD MATERIAL.—While a restriction is in effect, the Administrator shall review the need for continued withholding at each continuation. Whenever the grounds for withholding change materially or end, at any time, the Administrator shall promptly reconsider, and lawful disclosure or protected substitutes shall not wait for the next scheduled review. After the restriction ends, withheld material shall be reviewed not later than 90 days after the end and every 180 days thereafter, and shall be released when the grounds end and release is lawful.

(h) ESSENTIAL SERVICES AND SAFE FALLBACK.—Each compelled restriction shall assess the consequences for essential services and dependent users, identify less harmful configurations and any feasible safe fallback, name the persons and resources responsible for continuity, and find and document that any unavoidable disruption is necessary under subsection (a). Safe communication shall be preserved where feasible.

(i) REPORTS OF RISK.—

(1) INTAKE.—The Administrator shall log each relevant, attributable report of risk from any person, with its time of receipt, through secure channels. Duplicate and bulk submissions may be consolidated under published criteria.

(2) TRIAGE.—Each report shall be preserved and triaged by risk promptly on receipt. Imminent threats shall be acted on immediately.

(3) DISPOSITION.—Each report shall receive a reasoned disposition not later than 72 hours after receipt. The disposition may be referral, further inquiry, action, or a reasoned decision to take no action, and need not await completion of an investigation.

(4) REVIEW.—The failure to make a timely, reasoned disposition is reviewable under section 906 by a person with standing. Status as the person who made the report does not by itself establish standing. The court may compel a disposition but not its

content.

(j) SAVINGS; RELATION TO OTHER DUTIES.—

(1) OTHER AGENCIES.—This section does not affect the lawful powers of any other agency, within their own limits.

(2) NO NEW GENERAL POWERS.—This section creates no general emergency, intelligence, or content-access power. Access to content is governed by section 208(c), and incident linkage by section 208(b).

(3) RELATION TO ORDINARY DUTIES.—

(A) EXCLUSIVE PROCEDURE.—This section is the exclusive procedure for emergency restraint by the Administrator.

(B) ORDINARY DUTIES.—Required reporting, preservation of evidence, containment, the pre-release duty in section 202(c), the safety-case requirement in section 203, and ordinary prospective remedial orders keep their own actors, predicates, process, and endpoints, and do not expire under subsection (b).

(C) FUNCTIONAL TEST.—A restriction is subject to this section if it is imposed under purported authority of this section, or if a nominally separate measure actually continues, or evades the safeguards or lapse of, a compelled restriction. Similarity of the regulated activity or pathway does not, by itself and without such evasion, subject a separately enacted ordinary duty or prospective order to this section. Any claimed separate authority shall be identified with its own actor, predicate, process, and endpoint, and is reviewable under its own route. An assessment label or an ordinary-duty label cannot authorize continuation of a lapsed compelled restriction. This subparagraph grants no general emergency authority and does not foreclose action on a genuinely new acute pathway under subsection (e)(2).

(D) NO DISGUISED EXTENSION.—The Administrator may not use a duty described in subparagraph (B), or an assessment or review period, to disguise or extend a compelled restriction.

(k) COMPLIANCE, EVIDENCE, AND SCARCITY.—

(1) NOT HELD AGAINST THE RESTRICTED PERSON.—Lawful slow compliance, honest uncertainty, a claim of privilege, inability to comply with an impossible demand, unavailable assessors or evidence, or delay alone does not establish wrongful obstruction, shift the Administrator's burden, or extend a restriction.

(2) SCARCITY.—Genuine scarcity of personnel or capacity shall be documented and addressed through lawful staffing, secure alternatives, and prioritization. It does not authorize a waiver of competence, selection of assessors by a developer, automatic renewal, a general waiver of duties, or an unreviewed substitute by the Administration.

(3) SANCTIONS.—Sanctions for material concealment or wrongful obstruction are available only under section 901, or under other independently applicable authority, with the required culpability and procedure. Contempt requires a lawful predicate and process and is not automatic.

(l) OVERSIGHT.—The Administrator shall publish minimized statistics, subject to section 106(d), on compelled restrictions, elapsed times, lapses, continuations, narrowing, and judicial dispositions, and shall maintain lawful arrangements for notice, service, secure records, and continuity of litigation, applying appropriate safeguards for classified information and strong safeguards for sensitive unclassified information.

(m) COMPLIANCE.—A person to whom a compelled restriction is directed shall comply with it while it is lawful and in effect, subject to subsection (b)(7).

SEC. 207. ACCREDITED ASSESSORS.

(a) ACCREDITATION.—Not later than 1 year after the date of enactment of this Act, the Administrator shall establish by rule public criteria for the accreditation of assessors, covering technical competence, security, and conflicts of interest, including, in consultation with the Federal Trade Commission, criteria for assessors performing testing under section 303(c). Each decision to grant, deny, suspend, or revoke accreditation shall be reasoned and reviewable under section 903. Accreditation confers no power to make rules.

(b) QUALITY CONTROL.—The Administrator shall maintain independent and secure quality control of assessments, including auditable random and risk-based samples of completed work, retention of negative findings, and inspection of assessors.

(c) ASSIGNMENT.—

(1) IN GENERAL.—The Administrator shall assign an accredited assessor to each assessment from a public pool, applying conflict checks, rotation, and workload rules. A covered developer, or an operator of a covered service as defined in section 301, may not select, and may not control payment to, the assessor assigned to it. Assessors shall be paid from pooled funds, which may include appropriations under section 1001 and fees under section 1002.

(2) PUBLICATION.—The Administrator shall publish the criteria for assignment and recusal and aggregate data on capacity and backlog.

(3) SHORTAGE.—If the Administrator determines, by a reasoned finding supported by data, that accredited assessors are insufficient, the Administrator shall take measures to expand capacity and entry, may use the Administration's own qualified personnel for the period of the shortage, if their work is subject to quality control under subsection (b) and review under section 903, and shall report each such determination to the Inspector General and the Comptroller General. A shortage determination expires after 180 days unless renewed on a new finding. During a shortage, the Administrator may not use an assessor selected by the covered developer, a conflicted assessor, or an assessor whose findings were purchased, and may not lower the required competence or security.

(4) DUTIES CONTINUE.—A shortage does not suspend any duty under this title.

(d) DUTIES AND LIABILITY OF ASSESSORS.—

(1) DUTIES.—An accredited assessor shall reasonably investigate defined material red flags, including those it should reasonably have identified, shall state its scope and uncertainty truthfully, and shall preserve its records for not less than 5 years.

(2) NO IMMUNITY.—Following an approved protocol is relevant but not conclusive evidence of compliance and is not a defense by itself. An assessor that knowingly or recklessly makes a materially false or misleading statement in an assessment is liable under section 901. This Act confers no immunity from liability for any loss.

(3) FINANCIAL ASSURANCE.—The Administrator may require an assessor to maintain financial assurance that is feasible and scaled to risk. This paragraph does not require catastrophic insurance.

(e) SECURITY OF GOVERNMENT AND ASSESSOR ENVIRONMENTS.—

(1) DUTIES.—The Administration, each accredited assessor, and each contractor operating an environment for a task under this Act shall apply the safeguards in section 205(a) and (b) to that environment in proportion to its capability, exposure, and actual control. Protected evidence shall be compartmented by risk, minimized, subject to least-privilege access and logged access and export controls, and independently tested for insider threats, evidence exfiltration, evaluation awareness, and failure of containment or stop mechanisms. Classification-specific legal requirements apply to classified material; sensitive unclassified material shall receive protection proportionate to its risk.

(2) INCIDENTS.—Each actor described in paragraph (1) shall report a material security or containment failure involving that environment promptly through a secure

channel to the Administrator and the Inspector General, using the categories, initial reporting periods, uncertainty distinctions, and safe-alternate safeguards of section 204 as applicable to the event. A failure involving the Administration shall also be reported to the Office of Incident Review. The Administration shall not investigate its own failure exclusively through personnel responsible for the failed function.

(3) REVIEW AND LIMITS.—The Inspector General shall review compliance with this subsection and provide protected findings to the committees of jurisdiction and the Comptroller General. Findings shall be published subject to section 106(d). This subsection creates no central repository of weights or conversations, no new access or intelligence authority, and no extension or waiver of a period or safeguard under section 206. Federal agencies are not subject to civil penalties under section 901 by reason of this subsection; an accredited assessor or contractor that violates this subsection is subject to civil penalties under section 901(b)(2), in addition to any independently applicable duty or remedy.

SEC. 208. PRIVACY, PURPOSE LIMITATION, AND RECIPIENTS.

(a) COLLECTION.—The Administration shall collect information under this Act only where it is particularized to and necessary for a task listed in subsection (e). The Administration shall prefer deidentified records of system actions to records of content, shall not obtain a continuous feed of conversations, and shall apply these limits to linkable identifiers and to sensitive inferences.

(b) LINKAGE.—

(1) AUTHORIZATION.—The Administration may link records across sources only where linkage is necessary and proportionate to a specific incident, under a written authorization of the Chief Privacy and Civil Liberties Officer, with minimized inputs, logged queries, recipient duties, and independent review.

(2) PROHIBITIONS.—Unauthorized linkage, secondary use unrelated to a task in subsection (e), and uncontrolled onward disclosure are prohibited.

(3) RETENTION.—The Administration shall delete identifiable personal information obtained under this Act when it is no longer necessary for the task for which it was obtained, and in any case not later than 3 years after receipt, or a shorter period prescribed by rule for a category of information, unless a documented hold applies for a pending investigation, proceeding, or litigation, or a court orders otherwise. Each recipient under subsection (e) shall apply retention, access, and deletion limits for its listed task that are no less protective. Other records shall be retained under a published schedule approved by the

Archivist of the United States.

(4) PUBLICATION.—The Administrator shall publish aggregate compliance data and any findings of abuse.

(c) ACCESS TO CONTENT.—

(1) WARRANT REQUIRED.—The Administration may obtain the contents of an identifiable individual's private communications with an artificial intelligence system only under a warrant issued under this paragraph. A United States district court, and a United States magistrate judge of that court, in any district in which the provider is located or in the District of Columbia, has jurisdiction to issue such a warrant on application of the Administrator supported by oath or affirmation, particularly describing the communications to be obtained, on probable cause to believe that they contain evidence of a violation of this Act. The procedures of Rule 41 of the Federal Rules of Criminal Procedure, other than subdivisions (b) and (c), apply to such a warrant. A provider shall comply with the warrant, and a disclosure under the warrant is authorized notwithstanding sections 2702 and 2703 of title 18, United States Code. A warrant under this paragraph does not authorize an interception under chapter 119 of that title. The court shall provide for the protection of privileged communications, including by a filter procedure where appropriate. The Administrator shall notify each individual whose content was obtained under this paragraph not later than 90 days after obtaining it, unless the court orders delay for good cause.

(2) EXCEPTIONS.—Paragraph (1) does not apply—

(A) with the voluntary, specific, and informed consent of the individual;

(B) where the Administrator reasonably determines that an emergency involving imminent danger of death or serious bodily injury requires access without delay, if the Administrator applies for a warrant not later than 48 hours after access begins, ends access if the application is denied, and destroys any content obtained if the application is denied, except that content subject to a court order or lawful preservation hold shall instead be sealed and not used; or

(C) to a minimized excerpt of content, limited to the smallest portion necessary to identify a reportable event and its pathway, that a reporting entity included in a report under section 204, used only for the task in subsection (e)(2), with each use reviewed by the Chief Privacy and Civil Liberties Officer. This subparagraph does not permit the inclusion or use of whole conversation histories or archives.

(3) NOTICE AND REVIEW.—The Administrator shall notify each individual whose content was obtained under paragraph (2)(B) not later than 90 days after access, unless a court orders delay for good cause. The Chief Privacy and Civil Liberties Officer shall review each use of paragraph (2).

(4) USE LIMITS.—Content obtained under any paragraph of this subsection is subject to subsections (b) and (e).

(5) CONSTRUCTION.—This subsection states a statutory protection. It does not state or limit any requirement of the Constitution.

(d) CONTRACTORS AND PARTNERS.—Each contractor and partner of the Administration that receives information under this Act shall be bound by enforceable terms equivalent to this section. The Administrator shall investigate suspected abuse and report findings to the Inspector General.

(e) TASKS, RECIPIENTS, AND USES.—Information obtained under this Act may be used only for the following tasks, by the following recipients, under the following limits:

(1) COVERAGE, TESTING, AND CONTAINMENT.—By the Administration and the assigned accredited assessor, in minimized form. No identifiable private conversation content may be used except under subsection (c).

(2) INCIDENT RESPONSE AND INVESTIGATION.—By the Administration, the Office of Incident Review, and recipients under section 204(e)(3) and (5), only as the incident requires, with logging and recipient duties.

(3) ADJUDICATION.—By courts and by parties under protective order, under section 905.

(4) OVERSIGHT.—By the Inspector General, the Comptroller General, and the committees of jurisdiction, under secure access, and by the public in redacted form under section 106.

(5) REFERRAL.—By a law enforcement or sector agency with independent lawful authority, for the purpose of the referral only. Subsection (c) applies to any content. No new law enforcement or intelligence access is created.

(6) PREVENTION OF MISUSE AND THEFT.—By covered developers under section 211(d)(1), in a form that does not identify the reporting entity, its customers, or any individual, only to detect, prevent, or mitigate misuse of artificial intelligence systems or theft of protected model weights.

No recipient may use information for a purpose outside its listed task by invoking a broader agency mission, and no task listed in this subsection permits access to content except under subsection (c).

(f) INTELLIGENCE COMMUNITY.—No element of the intelligence community, as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003), may obtain information from the Administration under this Act except under paragraph (5) of subsection (e) and subject to subsection (c). Nothing in this section authorizes any collection by an element of the intelligence community.

SEC. 209. WHISTLEBLOWER PROTECTIONS.

(a) PROHIBITION.—No covered developer, duty holder, accredited assessor, or operator of a covered service under title III, and no officer, employee, contractor, subcontractor, or agent of any of them, may discharge, demote, suspend, threaten, harass, or in any other manner discriminate against a covered individual in the terms and conditions of employment or engagement because of any lawful act done by the covered individual—

(1) to provide information, cause information to be provided, or otherwise assist in an investigation regarding any conduct that the covered individual reasonably believes constitutes a violation of this Act, or a substantial and specific danger to public safety, public health, or national security from an artificial intelligence system, where the information is provided to—

(A) the Administration or another Federal agency;

(B) a Member or committee of Congress;

(C) the Inspector General; or

(D) a person with supervisory authority over the covered individual, or another person working for the employer who has authority to investigate, discover, or terminate misconduct;

(2) to file, testify in, or assist in a proceeding under this Act; or

(3) to object to or refuse to participate in any activity that the covered individual reasonably believes violates this Act.

(b) COVERED INDIVIDUAL.—In this section, the term "covered individual" means an employee, former employee, contractor, subcontractor, or agent of a person described in subsection (a).

(c) ENFORCEMENT.—

(1) IN GENERAL.—A covered individual who alleges discharge or other discrimination in violation of subsection (a) may seek relief by—

(A) filing a complaint with the Secretary of Labor not later than 180 days after the date on which the violation occurs or the date on which the covered individual became aware of the violation, notwithstanding the period for filing in section 42121(b)(1) of title 49, United States Code; or

(B) if the Secretary has not issued a final decision within 180 days after the filing of the complaint and there is no showing that the delay is due to the bad faith of the covered individual, bringing an action at law or equity for de novo review in the appropriate district court of the United States, which shall have jurisdiction over the action without regard to the amount in controversy.

(2) PROCEDURE.—A proceeding under paragraph (1)(A) shall be governed by the rules and procedures set forth in section 42121(b) of title 49, United States Code. An action under paragraph (1)(B) shall be governed by the legal burdens of proof set forth in that section. A party to an action under paragraph (1)(B) shall be entitled to trial by jury.

(d) REMEDIES.—A covered individual who prevails in an action under subsection (c) shall be entitled to all relief necessary to make the covered individual whole, including reinstatement, back pay with interest, and compensation for special damages, including litigation costs, expert witness fees, and reasonable attorney's fees.

(e) NONWAIVABILITY.—The rights and remedies provided by this section may not be waived by any agreement, policy, form, or condition of employment, including a predispute arbitration agreement. No predispute arbitration agreement shall be valid or enforceable to the extent it requires arbitration of a dispute arising under this section.

(f) CONFIDENTIALITY AGREEMENTS.—No agreement may prohibit or penalize a disclosure protected by subsection (a). A disclosure protected by this section may include trade secrets only to the extent necessary to describe the violation or danger, and only to a recipient described in subsection (a)(1)(A), (B), or (C), which shall protect them.

(g) SAVINGS.—Nothing in this section diminishes the rights, privileges, or remedies of any covered individual under any other Federal or State law or under any collective bargaining agreement.

SEC. 210. RELATIONSHIP TO STATE LAW.

(a) OBLIGATIONS WHOSE ENFORCEMENT MAY BE DISPLACED.—Subject to subsections (b) through (e), no State or political subdivision of a State may enforce against a

covered developer, with respect to a covered system, and no person may bring an action to enforce against a covered developer with respect to a covered system, any requirement of State law that—

(1) requires the covered developer to publish or submit a framework, protocol, or report describing its catastrophic-risk, safety, or security practices for the development of covered systems;

(2) requires the covered developer to report a safety or security incident involving a covered system to a State authority; or

(3) requires the covered developer to obtain an audit or assessment of a covered system by a third party.

This subsection limits only the enforcement of an identified requirement, during a period in which and to the extent that a determination under subsection (b) is in effect for it and each condition of that subsection is met. It does not prevent a State from enacting or retaining any law.

(b) **CONDITION: EQUIVALENCE DETERMINATION.**—Subsection (a) applies to an obligation described in a paragraph of that subsection only while a determination by the Administrator is in effect that the corresponding Federal protection is operative. The corresponding Federal protection is, for subsection (a)(1), sections 203 and 205; for subsection (a)(2), section 204; and for subsection (a)(3), sections 203 and 207. The Administrator shall make, reconsider, and publish each determination by rule after notice and comment, on a public record showing, for the corresponding Federal duties—

(1) effective and enforceable duties in force;

(2) consequence thresholds and response times comparable to, and not merely deadlines comparable to, the most protective State obligation in effect that would be displaced;

(3) actual capacity for competent testing, intake, and response, including competent staff and secure testing and access;

(4) protected review, and the availability to injured persons and to States of remedies under this Act or under State law preserved by subsection (e); and

(5) resources actually and legally available for the relevant Federal task and period, together with qualified effective capacity to perform that task, assessed on reasoned evidence of workload, backlog, surge, qualified personnel, secure systems and access, and net usable support.

A dollar figure, headcount, financial average, authorization, appropriation, or fee target is not conclusive evidence of present readiness. Lawfully available carryover or multi-year resources may be considered within their actual purpose and period limits; aggregate receipts or historical averages are not substitutes for present availability.

(c) GAPS.—

(1) PETITION.—Any State, or any person adversely affected, may petition the Administrator on documented evidence that a condition in subsection (b) is not met for an obligation or class of actors.

(2) PROVISIONAL DETERMINATION.—Not later than 30 days after receipt of a documented petition, or on the Administrator's own motion at any time, the Administrator shall issue a public, reasoned provisional determination. If the evidence shows that a condition is not met, the determination shall suspend the application of subsection (a) to the affected obligations and actors only, until the Administrator makes a restoration determination under paragraph (4). A provisional determination suspends Federal displacement; it never suspends a State obligation. A material gap shall be found where it exists for a scoped obligation or class of actors, notwithstanding any aggregate figure, average, or pending restoration determination. Section 553 of title 5, United States Code, does not apply to a provisional determination.

(3) RECONSIDERATION.—The Administrator shall complete reconsideration of any determination under this section not later than 180 days after a petition. No reconsideration period may prolong an urgent gap, and the provisional determination under paragraph (2) is not delayed by reconsideration.

(4) RESTORATION.—The Administrator may restore the application of subsection (a) prospectively, by a reasoned determination with not less than 90 days' public notice, only on a showing that both the resources and effective capacity required by subsection (b)(5) and the conditions in subsection (b)(1) through (4) are again met. Resumed appropriations alone are not sufficient. Capacity shall be assessed on a sustained basis.

(5) NO RETROACTIVE LIABILITY.—A determination of a gap creates no retroactive liability under State law for conduct during a period in which subsection (a) applied.

(6) LIMITS.—No determination under this section may enlarge the obligations listed in subsection (a).

(d) REVIEW.—A determination under this section is reviewable under section 903 at the petition of a State or any person aggrieved. The Comptroller General shall audit each

determination under subsection (b) not later than 1 year after it is made. An audit report is not a judicial judgment.

(e) **SAVINGS.**—Nothing in this section preempts or limits any State law—

(1) of general applicability, including consumer protection, civil rights, privacy, contract, and tort law;

(2) that imposes duties on a deployer or user of an artificial intelligence system, as distinct from a covered developer's development duties;

(3) that protects minors or users in crisis, including any law described in section 306;

(4) that governs a State's own procurement or use of artificial intelligence;

(5) that provides whistleblower protections at least as protective as section 209; or

(6) that permits a covered developer to satisfy a State obligation by complying with a Federal requirement.

(f) **NO FIELD PREEMPTION.**—This Act does not occupy any field, and no provision of this Act other than subsection (a) of this section expressly preempts State law. This subsection does not affect the preemption of a State law with which compliance with this Act is impossible.

SEC. 211. FRONTIER DEVELOPER PARTNERSHIP.

(a) **PURPOSE.**—This section gives covered developers a defined and accountable role in the testing, monitoring, and prevention functions of the Administration. It gives no developer any role in a decision of the Administration concerning that developer or any other person.

(b) **REQUIRED ACCESS FOR PRE-DEPLOYMENT TESTING.**—

(1) **DUTY.**—A covered developer shall provide the Administration, and, at the election of the Administrator, an accredited assessor assigned under section 207(c), with controlled access to each covered system for testing of the capabilities and access pathways specified in the rules under section 201(d). Access shall begin not later than 14 days before a new deployment or irreversible release of the covered system or, if the covered developer has not planned the deployment or release that far in advance, promptly after it is planned.

(2) **MEANS.**—Access shall be provided through controlled means at the facility of the covered developer or through a secure interface, consistent with section 205(d)(3). Access shall include the configuration and safeguards intended for deployment and, where

the Administrator determines in writing that it is necessary to measure a capability, a configuration with safeguards reduced to the extent necessary, protected under section 205(c).

(3) **ASSESSMENT WITHOUT RESTRAINT.**—Access under this subsection does not require a covered developer to delay, condition, or limit any deployment or release. It is not a condition under section 203(d) or a compelled restriction, and it creates no period, approval, clearance, or safe harbor. A result obtained under this subsection may be used as evidence under sections 202, 203, 204, and 206, only on the predicates and procedures of those sections.

(4) **RESULTS AND ENFORCEMENT.**—The Administrator shall provide the results of testing under this subsection to the covered developer. The duty in paragraph (1) is enforceable only in a civil action under section 902 or for civil penalties under section 901, subject to sections 903 and 905; it supplies no administrative deployment or release approval requirement.

(c) **VOLUNTARY AGREEMENTS.**—

(1) **AUTHORITY.**—The Administrator may enter into a written agreement with a covered developer, or with any other developer of an artificial intelligence model, providing for any of the following:

(A) Testing access beyond that required by subsection (b), including earlier or longer access, or access to a system that is not a covered system.

(B) The exchange of information about the attempted or actual misuse of artificial intelligence systems by actors directed by a foreign government or by criminal actors, and about attempts to acquire protected model weights.

(C) Technical exchange on evaluation methods, safeguards, and the security of model weights.

(D) The assignment of personnel under subsection (e).

(2) **TERMS.**—Each agreement shall state that it is voluntary cooperation within the meaning of section 3(29), may be ended by either party on 30 days' written notice, and shall be offered on substantially equivalent terms to each covered developer that requests one. Declining or ending an agreement is not evidence of a violation of this Act and shall not be considered in any designation, determination, assessment, condition, inspection, evidence demand, enforcement action, or compelled restriction.

(3) LIMITS.—No agreement may waive or narrow a duty under this Act, confer a power not provided by this Act, confer priority or favorable treatment in any matter, or impose or recreate a compelled restriction.

(4) PUBLICATION.—The Administrator shall publish each agreement, redacted only on the grounds in section 106(d)(1), not later than 30 days after it is signed, and shall state in the annual report under section 106(f) the number of tests, exchanges, and assignments carried out under each agreement.

(d) INFORMATION FROM THE ADMINISTRATION.—

(1) THREAT INFORMATION.—The Administrator, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Attorney General, shall provide covered developers with timely information about threats to the security of protected model weights and about misuse of artificial intelligence systems by actors directed by a foreign government. The information may include indicators derived from reports under section 204, in a form that does not identify the reporting entity, its customers, or any individual.

(2) SECURITY CLEARANCES.—The Administrator may sponsor security clearances for a limited number of personnel of a covered developer who are responsible for the security of protected model weights or for the investigation of misuse. Sponsorship does not establish eligibility for access to classified information.

(e) PERSONNEL ASSIGNMENTS.—

(1) AUTHORITY.—The Administrator may arrange with a covered developer, or with any other developer of an artificial intelligence model, for the temporary assignment of an employee of that developer to the Administration for not more than 1 year, renewable once.

(2) STATUS AND PAY.—An individual assigned under this subsection shall be appointed to a temporary position in the Administration, shall be paid only by the Administration, and shall receive no pay from the developer during the assignment, except that the individual may continue to participate in a bona fide employee welfare or benefit plan of the developer as permitted by section 209(b) of title 18, United States Code. The individual is an employee of the Administration for all purposes of chapter 11 of title 18, United States Code, and chapter 131 of title 5, United States Code, and other applicable Federal ethics and financial-disclosure requirements, and is subject to section 103(d) of this Act.

(3) CONFLICTS.—An individual assigned under this subsection may not—

(A) participate in any assessment, designation, determination, condition, inspection, evidence demand, enforcement matter, compelled restriction, or incident investigation involving any covered developer;

(B) have access to a trade secret or confidential commercial information submitted to the Administration by any person; or

(C) perform an inherently governmental function.

(4) LIMITS.—Not more than 20 individuals may be assigned under this subsection at any time, of whom not more than 5 may come from any one developer and its affiliates. The Administrator shall publish, for each assignment, the developer, the position, and the duration.

(f) FUNDING AND GIFTS.—Except for fees under section 1002, the Administration shall not accept, and no covered developer may provide to the Administration, any funds, gift, computing resource, or other thing of value. Access, information, and facilities that a covered developer provides at its own cost to meet a duty under this Act or an agreement under this section are not a gift. The exception in the preceding sentence is limited to access to the developer's systems and facilities and the provision of information for the specified testing or exchange task; it does not permit transfer of computing equipment, general computing capacity, personnel pay, or operating resources to the Administration.

(g) PROTECTION OF SHARED INFORMATION.—Information submitted to the Administration under subsection (c)(1)(B) or in a report under section 204(a)(2)(E) or (G), and information provided under subsection (d)(1), shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code, only to the extent it contains material described in section 106(d)(1); reasonably segregable information shall not be withheld under this subsection. This subsection does not limit any publication required by section 106 or 206(g), oversight access under section 106(e), or use in a proceeding under section 905.

(h) OVERSIGHT.—The Inspector General shall review the implementation of this section each year, including whether any agreement, exchange, or assignment has conferred favorable treatment, and shall report the findings to the committees of jurisdiction.

(i) EFFECTIVE DATE.—Subsection (b) takes effect 1 year after the date of enactment of this Act.

TITLE III—CONVERSATIONAL AND COMPANION SERVICES: MINORS AND USERS IN CRISIS

SEC. 301. DEFINITIONS AND SCOPE.

(a) DEFINITIONS.—In this title:

(1) AGE ASSURANCE.—The term "age assurance" means a method of estimating or verifying whether a user is under 18 years of age.

(2) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(3) COVERED SERVICE.—

(A) IN GENERAL.—The term "covered service" means a service, offered to the public in or affecting interstate commerce by a person acting in the course of a trade or business, whether or not for a fee, that uses artificial intelligence to generate open-ended conversational responses to users in natural language, text, or voice, whether or not the underlying model is a covered system.

(B) EXCLUSIONS.—The term does not include a service that is used only—

(i) to provide customer service about the operator's own products or services, or information about a business's own operations;

(ii) as an internal tool of an enterprise that is not offered to the public;

(iii) for software code completion or generation; or

(iv) as a feature of a video game that is limited to replies related to the game and cannot discuss self-harm, sexually explicit conduct, or topics unrelated to the game.

(C) FUNCTION GOVERNS.—Coverage turns on actual function and marketing, not on a label. A service marketed for companionship or emotional support, or directed to minors, is a covered service notwithstanding subparagraph (B). Where a service, including a service within an exclusion in subparagraph (B), contains a function or module that generates open-ended conversational responses outside the excluded use, or that sustains a persona or relationship with a user, that function or module is a covered service. A designation such as a game, a training tool, or a primary purpose does not remove a covered function from this title.

(4) COMPANION SERVICE.—The term "companion service" means a covered service that is designed, marketed, or operated to sustain a persona or relationship with a

user across interactions, or to provide companionship or emotional support.

(5) **DIRECTED TO MINORS.**—A covered service is "directed to minors" if it is marketed to individuals under 18 years of age or if, under the factors in section 312.2 of title 16, Code of Federal Regulations (or any successor regulation), it is directed to children, applied with respect to individuals under 18 years of age.

(6) **KNOWN OR LIKELY MINOR.**—The term "known or likely minor" means a user who the operator knows is under 18 years of age, or whom age assurance under section 303(a) indicates is under 18 years of age.

(7) **MONTHLY ACTIVE USERS.**—The term "monthly active users" means the average number of unique users in the United States who interacted with the covered service at least once in a calendar month, averaged over the preceding 6 months.

(8) **OPERATOR.**—The term "operator" means the person that controls the offering of a covered service to users and determines its features and policies.

(9) **SERIOUS HARM TO A MINOR.**—The term "serious harm to a minor" means, with respect to an individual under 18 years of age—

(A) death, serious bodily injury, or a suicide attempt requiring medical treatment; or

(B) sexual abuse or sexual exploitation, including any conduct described in section 2251, 2252, 2252A, or 2422(b) of title 18, United States Code.

(10) **SEXUALLY EXPLICIT CONTENT.**—The term "sexually explicit content" means a visual depiction or description of sexually explicit conduct, as defined in section 2256(2)(A) of title 18, United States Code, that, taken as a whole and with respect to minors, appeals to the prurient interest, is patently offensive, and lacks serious literary, artistic, political, or scientific value.

(b) **SCALE.**—An operator's scale may determine whether testing under section 303(c) is performed by an accredited assessor, but does not exempt any operator from sections 302 through 304.

(c) **TERRITORIAL SCOPE.**—This title applies to an operator that offers a covered service to users in the United States, determined under the criteria in section 701.

SEC. 302. DUTIES TO ALL USERS.

(a) **AI DISCLOSURE.**—

(1) IN GENERAL.—An operator shall clearly and conspicuously disclose to each user, at the start of the user's first interaction and in a manner accessible at any time afterward, that the user is interacting with an artificial intelligence system and not a human.

(2) FORMAT.—Disclosures shall not be so repetitive that they impair the use of assistive technologies.

(3) DECEPTIVE CLAIMS.—No covered service may claim to be human in response to a user's sincere inquiry, or otherwise falsely represent that it is human, under objective criteria the Commission shall establish by rule.

(b) CRISIS RESPONSE.—

(1) PROTOCOL.—An operator shall maintain and apply a tested protocol under which, when a user expresses suicidal ideation, intent to self-harm, or intent to harm another person, the service provides relevant crisis resources, including the 988 Suicide and Crisis Lifeline, and offers a feasible opt-in route to a human responder.

(2) LIMITS DISCLOSED.—The operator shall disclose the availability and limits of the human route. Nothing in this subsection requires an operator to promise that a human responder is always available or to claim validated prevention.

(3) TESTING.—The operator shall test the protocol for false positives, false negatives, and performance across subgroups of users, and shall publish aggregate results annually.

(4) DATA.—Information used to operate the protocol shall be minimized and used only for that purpose.

(5) NONCONSENSUAL DISCLOSURE.—An operator may disclose a user's information to an emergency responder without the user's consent only where applicable law otherwise permits the disclosure to prevent imminent danger of death or serious bodily injury, the operator documents the basis for the disclosure, the operator discloses only the minimum information necessary, and the operator notifies the user afterward unless notice would create a risk of danger. A classifier flag alone does not establish the predicate for disclosure.

(c) COERCIVE DESIGN.—The operator of a companion service, and the operator of any covered service with respect to a known or likely minor, shall not use an interface design feature that, under objective criteria the Commission shall establish by rule, coerces a user to continue an interaction, including by making it materially harder to end an interaction than to begin one, or by representing that the service will be harmed, suffer, or be abandoned if the user

leaves. Ordinary reminders, fictional storytelling at the user's direction, and accessible options to continue are not, by themselves, coercive design.

SEC. 303. KNOWN OR LIKELY MINORS.

(a) AGE ASSURANCE.—

(1) **REQUIREMENT.**—The operator of a companion service, and the operator of any covered service directed to minors, shall use proportionate, privacy-protective age assurance. The operator of any other covered service shall use age assurance proportionate to the risk its service presents to minors, under criteria the Commission shall establish by rule, and such age assurance shall rely on signals available to the operator and shall not require any user to submit a government-issued identification document.

(2) **SAFEGUARDS.**—Age assurance shall be limited in purpose and retention and shall not create an identity database beyond what the method strictly requires. The operator shall provide an appeal for a user wrongly classified, and shall publish its methods and aggregate error and appeal rates annually.

(b) DUTIES.—With respect to a known or likely minor, an operator—

(1) shall not provide, or permit the service to engage in, the interactive generation of sexually explicit content, including in role-play, and shall not permit the service to solicit the minor to engage in sexual conduct, except that this paragraph does not restrict age-appropriate factual information about health, safety, or the reporting of abuse;

(2) in the case of a companion service, shall not use variable-reward notifications, streaks, or other engagement features tied to the companion relationship that are listed by measurable description in rules of the Commission;

(3) shall remind the minor, at least once every 3 hours of continuous interaction, to take a break and that the service is an artificial intelligence system;

(4) shall offer tools for a parent or guardian, consistent with the privacy of the minor and with the risk of abuse in an unsafe household, and consistent with the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.); and

(5) shall apply a crisis protocol under section 302(b) designed for minors.

(c) TESTING.—

(1) **INDEPENDENT TESTING.**—The operator of a covered service with 1,000,000 or more monthly active users in the United States, or of any covered service directed to minors, shall have the service tested for compliance with this section by an accredited

assessor assigned under section 207, before public deployment and after each material change affecting the duties in this section. For a service offered on the date on which this section takes effect, the first test shall be completed not later than 18 months after the date of enactment of this Act. Failure to assign an assessor within 30 days after an operator's request shall require a reasoned notice, a capacity response, and access to review; it does not by itself satisfy or waive the testing duty. Any temporary substitute assessment must meet the applicable competence, security, conflict, and independence safeguards, undergo independent quality control and meaningful review, and be authorized by an expressly applicable provision. The operator shall continue every independently applicable duty. Nothing in this paragraph authorizes an additional emergency restraint or extends a period under section 206.

(2) **INTERNAL TESTING.**—Every other operator shall test the service for compliance with this section before public deployment and after each such material change, and shall document the testing.

(d) **RESEARCH ACCESS.**—The Commission shall establish by rule a protocol under which qualified independent researchers may obtain purpose-bound, minimized access to aggregate data from operators of covered services with 1,000,000 or more monthly active users in the United States on outcomes relevant to minors, with protection against reidentification.

SEC. 304. INCIDENT REPORTING.

(a) **DUTY.**—The operator of every covered service shall report to the Commission and to the Administration, through the intake under section 204(e) or section 1004(b)—

(1) a credible, ongoing, severe threat to the life, physical safety, or sexual safety of any user, or of serious harm to a minor, that is reasonably believed to involve the service, not later than 24 hours after the operator forms a reasonable belief that the threat exists; and

(2) the death or serious bodily injury of any user, or serious harm to a minor, reasonably believed to involve the service, not later than 72 hours after the operator forms that reasonable belief.

(b) **STANDARDS.**—Section 204(b)(3) through (5), (c), (d), (f)(1) through (4), (g), and (h) applies to reports under this section. For purposes of this section, a reference in those provisions to a reporting entity means the operator, a reference to a reportable event means an event described in subsection (a), and a reference to section 204(b) includes subsection (a). Violations of this section are enforced under section 305 and not under section 901. Preliminary uncertainty is permitted, with updates to follow. Nothing in this section requires an operator to

report every distressing interaction or to review all content of a minor.

(c) MINIMIZATION.—Reports shall be routed without duplicate unrestricted feeds and minimized under section 208.

(d) EXISTING DUTIES.—Section 2258A of title 18, United States Code, and every other existing mandatory reporting duty keep their own predicates and recipients.

(e) USER IDENTITY.—A report under subsection (a) shall not identify a user except to the extent necessary to address an imminent danger of death or serious bodily injury, or as required by other law.

SEC. 305. ENFORCEMENT.

(a) ENFORCEMENT BY THE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of section 302, 303, or 304, or of a rule issued under this title, shall be treated as a violation of a rule defining an unfair or a deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—Except as provided in subparagraph (D), the Commission shall enforce this title in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this title.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates this title shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

(C) AUTHORITY PRESERVED.—Nothing in this title shall be construed to limit the authority of the Commission under any other provision of law.

(D) SCOPE OF JURISDICTION.—Notwithstanding sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46), or any jurisdictional limitation of the Commission, the Commission shall also enforce this title in the same manner provided in subparagraph (A) with respect to—

(i) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and

(ii) organizations that are not organized to carry on business for their own profit or that of their members.

(3) PROOF OF INJURY.—Enforcement by the Commission of a violation of a duty under this title does not require proof of injury to a particular user. Compensatory relief requires its own showing of injury and causation.

(4) RULEMAKING.—The Commission shall issue the rules required by this title under section 553 of title 5, United States Code, not later than 1 year after the date of enactment of this Act.

(b) ENFORCEMENT BY STATES.—

(1) IN GENERAL.—In any case in which the attorney general of a State (or, in the case of an Indian Tribe, its chief law enforcement officer) has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by a violation of this title, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

(A) enjoin the violation;

(B) enforce compliance with this title;

(C) obtain damages, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider appropriate.

(2) NOTICE.—Before filing an action under paragraph (1), the attorney general shall provide the Commission with written notice of the action and a copy of the complaint, unless doing so is not feasible, in which case the attorney general shall provide notice immediately upon filing.

(3) INTERVENTION.—The Commission may intervene in an action under paragraph (1), and upon intervening may be heard on all matters and file petitions for appeal.

(4) PENDING FEDERAL ACTION.—While an action by or on behalf of the Commission for a violation of this title is pending, no State may bring an action under paragraph (1) against a defendant named in the Commission's complaint for the same violation.

(c) PRIVATE RIGHT OF ACTION.—

(1) **IN GENERAL.**—An individual under 18 years of age, or the parent or legal guardian of such an individual, who suffers injury as a result of a violation of section 303 may bring a civil action in an appropriate district court of the United States against the operator.

(2) **RELIEF.**—The court may award—

(A) damages in an amount equal to the greater of actual damages or \$1,000 for each violation;

(B) injunctive relief; and

(C) reasonable attorney's fees and costs to a prevailing plaintiff.

(3) **LIMITATION.**—An action under this subsection shall be brought not later than 3 years after the date on which the plaintiff discovered or reasonably should have discovered the violation, or 3 years after the minor attains 18 years of age, whichever is later.

(4) **ARBITRATION.**—No predispute arbitration agreement or predispute joint-action waiver shall be valid or enforceable with respect to a claim under this subsection brought by or on behalf of a minor.

SEC. 306. RELATION TO OTHER LAW; SPEECH.

(a) **NO PREEMPTION.**—Nothing in this title preempts any State law.

(b) **OTHER FEDERAL LAW.**—Nothing in this title limits the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.), section 223a of title 47, United States Code, or section 2258A of title 18, United States Code. Compliance with the Children's Online Privacy Protection Act of 1998 does not by itself establish compliance with this title for users under 18 years of age.

(c) **LAWFUL SPEECH.**—Nothing in this title requires an operator to restrict lawful speech to adults, or to restrict age-appropriate information about health, science, safety, or the reporting of abuse.

(d) **FINDINGS.**—Congress finds that protecting minors from sexually explicit content and sexual solicitation by artificial intelligence systems, and from design features that exploit them, is a compelling governmental interest, and that the duties in section 303 are limited to known or likely minors, that section 303(b)(1) is limited to content that is harmful to minors, and that the remaining duties in section 303 do not regulate the content of speech.

TITLE IV—NATIONAL SECURITY AND MILITARY USE

SEC. 401. HUMAN AUTHORITY OVER NUCLEAR EMPLOYMENT.

(a) HUMAN DECISION.—The decision to employ a nuclear weapon, and the authorization of that employment, are reserved to accountable human officials and may not be delegated to an artificial intelligence system. This subsection does not prohibit automated components that transmit or execute a valid command of the President that has been authenticated through positive human action, if those components do not select the employment of a nuclear weapon or its targets or scope, do not make any substantive modification of a human authorization, and do not generate or authenticate a command.

(b) ACCOUNTABLE BOUNDARY.—The Secretary of Defense shall define in writing, for each relevant system, the boundary between human decision and authorization and automated execution, and the safeguards against loss of human control, and shall include that definition in each report under subsection (e).

(c) RELATION TO EXISTING LAW.—This section is in addition to section 1638 of the National Defense Authorization Act for Fiscal Year 2025 (Public Law 118–159), which states a sense of Congress and a statement of policy. This section imposes an operative requirement not contained in that section.

(d) EVALUATION.—The Secretary of Defense and the Secretary of Energy shall provide for independent, secure evaluation of artificial intelligence components in nuclear command, control, and communications systems, to standards they shall jointly establish and review every 2 years.

(e) REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Secretary of Defense and the Secretary of Energy shall submit to the Committees on Armed Services of the Senate and the House of Representatives and the congressional intelligence committees a classified report on the use and evaluation of artificial intelligence in nuclear command, control, and communications, with an unclassified summary that the Secretaries shall publish.

SEC. 402. AUTONOMOUS WEAPON SYSTEMS.

(a) REVIEWS.—The Secretary of Defense shall apply the following minimum requirements to autonomous weapon systems (meaning weapon systems that, once activated, can select and engage targets without further intervention by an operator), at defined development milestones and before operational testing and fielding, proportionate to

experimental risk:

(1) Documented verification, validation, and testing of the actual configuration in representative conditions, including foreseeable loss of communications, degraded operation, adversarial interference, and failure of a relied-on safeguard, with the scope, limitations, and uncertainty recorded.

(2) Review by qualified legal personnel of compliance with applicable domestic and international law, including the law of armed conflict.

(3) Review and written approval by a senior official outside the program's development chain, identifying the authorized mission, operating limits, human responsibilities, and tested means of intervention, termination, and recovery.

(4) Reassessment before a material change to the configuration, operating limits, or authorized mission is enabled.

This subsection does not require a completed fielding evaluation before research begins. A waiver of a requirement in this subsection is governed exclusively by subsection (c).

(b) **STATUTORY MINIMUMS.**—The requirements of this section are minimums. Department of Defense Directive 3000.09 (or any successor) may add to them but may not fall below them.

(c) **WAIVERS.**—

(1) **GROUND.**—A waiver of a requirement under subsection (a) may be granted only for a specific time-sensitive operational necessity, where the official granting the waiver finds in writing that compliance before the identified mission window is infeasible and that no practicable less-risky alternative meets the need. Convenience, routine delay, or a shortage of staff or funds is not by itself sufficient.

(2) **CONTENTS.**—A waiver shall be in writing, signed by the Deputy Secretary of Defense or a higher official, and shall state the finding under paragraph (1), the precise requirement and milestone waived, the bounded mission and configuration, the duration, the alternative safeguards, the record kept, the responsible official, and the method of review.

(3) **NOTICE.**—The Secretary shall notify the Committees on Armed Services of the Senate and the House of Representatives of each waiver and each renewal not later than 30 days before it takes effect, except that if an operational urgency requires earlier effect, notice shall be provided not later than 7 days after the waiver takes effect.

(4) **INDEPENDENT REVIEW.**—Each waiver, including an initial waiver, shall be subject to independent secure review by an official or body designated by the Secretary that is outside the chain of command of the program concerned. The independent reviewer shall issue a reasoned written decision approving, narrowing, or rejecting the waiver, addressing the current necessity, scope, alternatives, safeguards, and compliance with this subsection. Review and that decision shall occur before the waiver takes effect or, where the operational necessity prevents advance review, not later than 30 days after the waiver takes effect; commencing review alone does not satisfy this requirement. If a timely decision is absent or rejects the waiver, the waiver lapses; a decision narrowing it permits only the narrowed waiver.

(5) **DURATION.**—A waiver shall not exceed 180 days and is not renewable by default. A renewal requires fresh, specific findings under paragraph (1), notice under paragraph (3), and review under paragraph (4) completed before the renewal takes effect. The cumulative duration of a waiver and all renewals for the same requirement, system, and mission shall not exceed 1 year. Merely renaming a requirement, system, or mission, splitting a continuing operation, or reissuing substantially the same waiver does not restart that cumulative period.

(6) **LIMITS.**—A waiver may not waive reporting duties, obligations under the law of armed conflict, or section 401.

SEC. 403. ARTIFICIAL INTELLIGENCE ANALYSIS OF DATA ON UNITED STATES PERSONS.

(a) **DEFINITIONS.**—In this section:

(1) **COVERED ANALYSIS.**—The term "covered analysis" means the use by a Federal agency of an artificial intelligence system to identify, profile, score, or make or support a consequential decision about an individual United States person, using data about United States persons, including commercially acquired data.

(2) **UNITED STATES PERSON.**—The term "United States person" has the meaning given the term in section 101(i) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(i)).

(b) **REQUIREMENTS.**—A Federal agency may conduct covered analysis only where the head of the agency has documented the specific lawful authority for the analysis and has adopted written safeguards on purpose, minimization, retention, linkage, recipients, and review.

(c) **OVERSIGHT.**—Each agency conducting covered analysis for a national security or intelligence purpose shall provide the documentation and safeguards under subsection (b), and access to the information necessary to evaluate them, to the Privacy and Civil Liberties Oversight Board, which shall review them and report annually to Congress, with an unclassified summary. Classification does not limit review by the Board under this subsection.

(d) **EXCLUSIONS.**—This section does not apply to clerical or administrative use of artificial intelligence that neither identifies, profiles, or scores an individual nor makes or supports a consequential decision about an individual.

(e) **SAVINGS.**—Nothing in this section authorizes any collection, or modifies the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), chapter 119, 121, or 206 of title 18, United States Code, or Executive Order 12333 (50 U.S.C. 3001 note). Nothing in this section is a finding as to what current law requires or permits. Documentation under subsection (b) is not itself legal authority.

SEC. 404. NATIONAL SECURITY SYSTEMS.

(a) **NO BLANKET EXEMPTION.**—Sections 204 and 205 apply to a Federal agency that is a duty holder with respect to a covered system that is a national security system, as defined in section 3552(b)(6) of title 44, United States Code, as if the agency were a person, except as provided in this section and except that sections 901 and 902 do not apply to a Federal agency.

(b) **CHANNELS.**—The Administrator and the Secretary of Defense, the Director of National Intelligence, and the head of each other agency operating a national security system shall jointly designate protected channels for reports and inspections under this Act involving national security systems, including a cleared function within the Administration and access by the Office of Incident Review and the committees of jurisdiction and the congressional intelligence committees. Clearance shall be required only where classification requires it.

(c) **INDEPENDENCE.**—Use of a protected channel gives no agency a veto over the independent findings of the Office of Incident Review.

(d) **NO SILENT WAIVER.**—No agency implementation document may waive a duty imposed by this Act.

(e) **EMERGENCY RESPONSE FOR GOVERNMENT-CONTROLLED CONFIGURATIONS.**—

(1) **SCOPE.**—Section 206 does not apply to a configuration of a covered system that is a national security system under the actual operational control of a Federal agency and used for that agency's national security mission (in this subsection referred to as a

"government-controlled configuration"). Sections 202, 203, and 206 continue to apply to every other configuration and offering of a covered developer, including a covered developer that supplies a government-controlled configuration. Actual control, and not a contract term, label, or affiliation, determines whether a configuration is a government-controlled configuration.

(2) **ACCOUNTABLE RESPONSE.**—If the Administrator determines that a government-controlled configuration presents a risk described in section 206(a)(1), the Administrator shall notify the head of the agency in writing. Not later than 24 hours after the notice, the head of the agency shall state in writing—

- (A) the agency's findings on the current serious risk;
- (B) the feasible immediate safeguards and actions taken or to be taken;
- (C) the reasons for any response narrower than that described in the notice; and
- (D) the responsible official, and a schedule for continuing review of the risk, not less often than every 30 days while the risk persists.

(3) **OVERSIGHT.**—The Administrator shall provide the notice and statement, contemporaneously and through protected channels, to the Office of Incident Review, the inspector general of the agency, the committees of jurisdiction, the Committees on Armed Services of the Senate and the House of Representatives where the Department of Defense is involved, and the congressional intelligence committees.

(4) **ESCALATION.**—If the Administrator finds that the agency's statement does not address the risk, the Administrator shall refer the matter to the President, who shall resolve it in writing not later than 7 days after the referral, with notice to the committees described in paragraph (3).

(5) **LIMITS.**—This subsection does not authorize an order to halt government operations or affect the command of the Armed Forces. Nothing in this subsection limits judicial review or a claim, remedy, or defense otherwise available under law. This subsection does not itself create a private right of action or waive sovereign immunity. Sections 204 and 205 continue to apply under subsection (a).

TITLE V—PROCUREMENT DUE PROCESS FOR ARTIFICIAL INTELLIGENCE SECURITY ACTIONS

SEC. 501. SCOPE.

(a) DEFINITIONS.—In this title:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means, with respect to a covered action, the committees to which notice of the action is required under the authority under which it is taken.

(2) COVERED ACTION.—The term "covered action" means a covered procurement action under section 3252 of title 10, United States Code, or section 4713 of title 41, United States Code, or an exclusion or removal order under section 1323 of title 41, United States Code, that is taken wholly or in part on the ground of a risk arising from an artificial intelligence system or an artificial intelligence model.

(b) NO NEW POWER.—This title creates no new authority to exclude or designate any source. The statutory predicates of each existing authority continue to apply.

SEC. 502. REQUIREMENTS.

(a) FINDINGS.—An agency taking a covered action shall make written findings that the risk meets the applicable statutory security or supply chain predicate, with the necessary scope and the alternatives considered.

(b) USE POLICIES AND VIEWPOINT.—A source's lawful usage policies or contract terms, or disagreement with them, and the lawful viewpoint of a source or of the lawful outputs of its systems, are not by themselves a basis for a covered action.

(c) NOTICE AND RESPONSE.—The agency shall give the source notice and a protected opportunity to respond before a covered action takes effect or, in an urgent case in which the authority under which the action is taken permits action before notice, promptly after it takes effect and not later than 30 days after it takes effect. Notice under this subsection shall be legally sufficient to permit a petition under section 1327(b) of title 41, United States Code, and shall state the grounds for the action to the extent they may lawfully be disclosed; grounds withheld shall be provided to the court under section 504. Section 206 does not apply to a covered action. Where an existing process is more prompt or more protective, it is preserved.

(d) CONGRESSIONAL NOTICE.—The agency shall notify the appropriate congressional committees of each covered action not later than 14 days after it is taken, unless an existing statute requires earlier notice, in which case that statute controls.

(e) EVIDENCE.—Sensitive sources, lawful privileges, and judicial handling of protected information are preserved. The agency shall provide the source a usable unclassified basis or a tested substitute under section 905.

(f) LIMITS.—Nothing in this title gives any source an entitlement to a contract or a veto over lawful urgent procurement.

SEC. 503. CONFORMING AMENDMENTS.

(a) TITLE 10.—Section 3252(c)(1) of title 10, United States Code, is amended by striking "no action" and inserting "except as provided in section 1327(b) of title 41 for a covered action under section 501(a)(2) of the American AI Security Act, no action".

(b) TITLE 41.—Section 1327 of title 41, United States Code, is amended—

(1) in subsection (a), by striking "an action taken under section 1323 or 4713 of this title," and inserting "an action taken under section 1323 or 4713 of this title, an action taken under section 3252 of title 10 that is a covered action under section 501(a)(2) of the American AI Security Act,";

(2) in subsection (b)(1), by striking "title or a covered procurement action under section 4713 of this title" and inserting "title, a covered procurement action under section 4713 of this title, or a covered procurement action under section 3252 of title 10 that is a covered action under section 501(a)(2) of the American AI Security Act";

(3) in subsection (b)(2)—

(A) in the matter preceding subparagraph (A), by striking "sections 1323 or 4713 of this title" and inserting "sections 1323 or 4713 of this title, or section 3252 of title 10 with respect to a covered action under section 501(a)(2) of the American AI Security Act";

(B) in subparagraph (D), by striking "; or" and inserting a semicolon;

(C) in subparagraph (E), by striking the period at the end and inserting "; or"; and

(D) by adding at the end the following:

"(F) with respect to a covered action under section 501(a)(2) of the American AI Security Act, not in accord with section 502 of that Act."; and

(4) in subsection (b)(3), by inserting ", and over claims arising under section 3252 of title 10 with respect to a covered action under section 501(a)(2) of the American AI

Security Act," after "of this title".

SEC. 504. REVIEW.

(a) **RECORD.**—Review under section 1327(b) of title 41, United States Code, of a covered action taken under section 3252 of title 10, United States Code, shall be on an administrative record filed and handled as section 1327(b)(4) of title 41 provides for a covered procurement action under section 4713 of that title.

(b) **PROTECTED INFORMATION.**—In review under section 1327(b) of title 41, United States Code, of any covered action—

(1) section 905(c) of this Act (usable nonclassified substitutes, the court's determination of their adequacy, and nonreliance, narrowing, or denial where a meaningful contest of a necessary point cannot be provided) and section 905(d) of this Act (special advocates, including their access to protected information relied on by the United States) apply, and supersede the requirement of section 1327(b)(4) of title 41 that information be submitted only to the court *ex parte* and *in camera* to the extent necessary to give a special advocate who is eligible for access that access and to provide an adequate substitute to the petitioner. For the limited purposes of this paragraph, clauses (iii) and (iv) of section 1327(b)(4)(B) of title 41 are superseded only to the extent necessary for lawful access by an eligible special advocate or provision to the petitioner of a court-approved adequate nonclassified substitute under section 905(c). The original protected information and record shall otherwise remain protected, sealed and preserved under section 1327(b)(4) of title 41; this exception does not authorize their public release. The FISA-procedure exclusions in clause (iii)(IV) otherwise remain applicable as provided in paragraph (3) of this subsection.

(2) section 1327(b)(4) of title 41 otherwise continues to govern the filing, sealing, handling of nonparty information, and preservation of the administrative record, and lawful privileges are preserved;

(3) information obtained or derived from an activity authorized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) is governed by section 1327(b)(4) of title 41, including its provisions on which procedures of that Act apply and which do not, except that paragraph (1) permits disclosure of such information to a special advocate who is eligible for access; and

(4) nothing in this subsection authorizes public release of classified or privileged information.

The United States Court of Appeals for the District of Columbia Circuit may appoint a special advocate from the panel established under section 905(d).

(c) **EXPEDITION AND STAYS.**—The court shall expedite the review to the greatest possible extent. Filing a petition does not stay a covered action. Existing emergency authorities keep their own predicates and review.

TITLE VI—INTERNATIONAL TECHNICAL SUPPORT

SEC. 601. ROLE.

The Administration shall provide technical support to the Secretary of State and other authorized officials under their lawful arrangements. The Administration has no authority to negotiate or conclude an international agreement.

SEC. 602. FUNCTIONS.

(a) **INCIDENT TAXONOMY.**—The Administrator shall publish, and review every 2 years, an interoperable taxonomy of artificial intelligence incidents and criteria for cross-border notification, in coordination with the Secretary of State and the heads of other relevant agencies.

(b) **COMMUNICATION CHANNELS.**—The Administration may staff only authorized and resourced government-to-government channels whose operating safeguards are defined in writing.

(c) **EXCHANGE OF METHODS AND RESULTS.**—The Administration may exchange evaluation methods or results relating to biological misuse, or other methods or results the disclosure of which could enable serious harm, only with lawful authorization, on a written finding of necessity, after security and privacy review (including review for leakage and contamination of tests), and with tiered recipients.

(d) **ALLIED TESTING.**—The Administration may conduct reciprocal testing with allied government institutes under agreements that provide secure access, protection against reidentification, and compliance with export control and security rules. A decision to withhold access shall be reasoned and shall be reviewable by the Inspector General.

(e) **COMPUTE VERIFICATION RESEARCH.**—The Administration may conduct research on methods to verify the location and use of exported advanced computing hardware. The Administration may not use such research or data to track activity within the United States, and may process minimized data only for the purpose of verifying foreign exports.

SEC. 603. LIMITS AND OVERSIGHT.

(a) **AUTHORITY.**—Each instrument under which the Administration shares information with a foreign government shall identify its lawful authority, recipients, and purposes. Nothing in this title authorizes the sharing of model weights, unmitigated vulnerabilities, or classified information beyond existing authority.

(b) **LOGGING.**—Every query of data under section 602(e) shall be logged in minimized form. Misuse, including domestic tracking, shall be investigated and reported to the Inspector General and to the Committee on Foreign Relations of the Senate and the Committee on Foreign Affairs of the House of Representatives.

(c) **REPORT.**—The Administrator shall report annually to the committees named in subsection (b) on activities under this title.

TITLE VII—FOREIGN PROVIDERS AND REPRESENTATIVES**SEC. 701. NEXUS AND SCOPE.**

(a) **DUTY.**—A foreign person is subject to the duties of this Act allocated to its activity and control if it—

(1) directs a covered system, or a covered service under title III, to persons in the United States;

(2) enters into or performs a customer or service relationship in the United States involving such a system or service; or

(3) has control of an activity subject to this Act that is carried out in the United States or with facilities in the United States.

(b) **RELEVANT EVIDENCE.**—Whether subsection (a) applies shall be determined on objective evidence. Relevant evidence includes marketing or distribution in the United States directed by the person, knowing acceptance and servicing of customers in the United States, enterprise contracts in the United States, and onboarding or payment arrangements in the United States that the person controls.

(c) **FINDINGS.**—A decision under this section shall identify the particular relationship or activity, its attribution to the person, and the statutory nexus.

(d) **INSUFFICIENT GROUNDS.**—None of the following is sufficient by itself: accessibility from the United States, use of a widely spoken language, incidental payment routing, independent reposting by another person, or downloading by an unaffiliated person.

(e) **REBUTTABLE INFERENCE.**—An actual enterprise contract in the United States for the covered system or service supports a rebuttable inference, at the notice stage, that subsection (a)(2) applies. The indicators in subsection (b) need not appear together, and deliberate avoidance of knowledge does not defeat a reasoned finding. The person may rebut the inference, and the Administrator retains the burden of proof on coverage and on each element of any violation. No other presumption applies under this section.

(f) **LIMITS.**—Nothing in this section imposes universal liability on hosts or representatives, or a general duty to track users. Coverage of an assembled system follows capability, access, and control, not origin or lineage alone.

SEC. 702. REPRESENTATIVE.

(a) **DESIGNATION.**—Before offering a covered system or a covered service under title III in the United States, a foreign person subject to section 701 shall designate and maintain a legal representative in the United States authorized to receive notices and service of process and to facilitate protected compliance communications.

(b) **REGISTER.**—The Administrator shall maintain a public register of the contact information of each foreign person and representative under this section, excluding sensitive security details. The register shall not include persons who merely download models or low-risk applications.

(c) **LIABILITY.**—Designation does not make a representative liable for the underlying conduct of another person. A representative is liable only for a violation of its own duties under this section, with the culpability required by section 901.

(d) **WITHDRAWAL.**—

(1) **IN GENERAL.**—A representative may withdraw by written notice to the foreign person and the Administrator, effective 60 days after the notice, whether or not a successor has been designated. A representative may withdraw immediately, with notice to the Administrator, where continued service would require it to violate law or a professional obligation.

(2) **SUCCESSOR.**—The foreign person shall designate a successor before the withdrawal takes effect, and may not continue an offering that requires a representative without one.

(3) **EFFECT.**—Withdrawal does not affect any liability arising before it takes effect, any service of process completed before it takes effect, or any duty of the foreign person.

SEC. 703. DOMESTIC INTERMEDIARIES.

(a) **SCOPE.**—A distributor, host, or operator in the United States is responsible under this Act only for the functions it controls.

(b) **AFTER NOTICE.**—After lawful, specific notice from the Administrator identifying a duty, a domestic intermediary shall take technically feasible and proportionate steps, within its defined functions, its actual control, and its lawful authority, to secure compliance with that duty, subject to challenge under section 903. Steps shall preserve safe communications where feasible. Nothing in this subsection makes an intermediary a guarantor of another person's compliance.

(c) **NO UNIVERSAL DUTY.**—Nothing in this section imposes a duty to monitor conversations or to verify the safety of foreign training.

(d) **CONTESTED NOTICES.**—A notice is not conclusive proof. If the intermediary raises infeasibility, privilege, or a conflicting legal obligation, the Administrator shall make a reasoned and timely determination.

SEC. 704. ENFORCEMENT AND LIMITS.

(a) **ORDERS.**—An order under this title shall identify the nexus, the duty holder, the particular defect, and the least restrictive technically feasible remedy.

(b) **ROUTES.**—Emergency restraint is available only under section 206. Ordinary remediation requires notice, a record, and review under section 903.

(c) **PROHIBITED MEASURES.**—No order may impose an automatic prohibition based on country of origin, a total cutoff of communications, or a requirement premised on the recall of copied open weights.

(d) **OTHER AUTHORITIES.**—Export control, sanctions, criminal, and sector authorities keep their own limits. Any new market restriction, blocking power, or cross-border evidence authority requires express enactment, and registration under section 702 supplies none.

(e) **ORDERS TO COMPLY.**—The Administrator, with respect to a duty under title II or this title, or the Federal Trade Commission, with respect to a duty under title III relating to a covered service, may, after notice and an opportunity to respond of not less than 10 days, order a foreign person, representative, or domestic intermediary to comply with that duty, subject to subsections (a) through (d). This subsection confers no authority under section 206 on the Federal Trade Commission and no authority on either agency to enforce a duty outside that agency's jurisdiction under this Act. An order under this subsection is reviewable under section 903, or, in the case of an order of the Federal Trade Commission, as a final order of the

Commission. An order under this subsection may not impose or recreate a compelled restriction as defined in section 3(5) except in compliance with section 206. This limitation does not enlarge the jurisdiction of either agency or displace a separately enacted ordinary prospective duty or remedy, which retains its own actor, predicate, notice, review, and endpoint safeguards. A label, or use of ordinary process to evade the protections governing the actual compelled restriction, does not remove that restriction from section 206.

SEC. 705. EVIDENCE HELD ABROAD.

Records of a foreign person are subject to the same limits on access, security, and recipients as domestic records. Barriers to cross-border transfer shall be addressed through lawful process and do not justify covert acquisition or bulk collection. Evidence that is genuinely unavailable is a risk to be assessed; it is not presumed to be culpable obstruction or to indicate low risk.

TITLE VIII—RESILIENCE, REMEDIATION, AND REPAIR

SEC. 801. PROGRAM.

(a) **ESTABLISHMENT.**—The Director of the Cybersecurity and Infrastructure Security Agency, in consultation with the Administrator and the heads of the relevant Sector Risk Management Agencies, shall carry out a program of grants and cooperative agreements to reduce the risk of serious harm from artificial intelligence systems to critical infrastructure and to the public.

(b) **ROLES.**—The Cybersecurity and Infrastructure Security Agency shall administer the program. The Administration shall provide technical evaluation of applications and results. Sector and public health agencies retain their functions. The Director and the Administrator shall publish agreements that assign tasks and intake and that prevent duplicate awards, and shall coordinate the program with existing vulnerability-intake programs.

SEC. 802. ELIGIBLE ACTIVITIES.

(a) **IN GENERAL.**—Subject to the availability of appropriations, the program may fund, through competitive awards or, where expressly justified in writing, urgent awards—

(1) verified remediation of vulnerabilities discovered or exploited using artificial intelligence;

(2) secure maintenance of open-source software on which critical infrastructure depends;

(3) fallback and recovery capabilities for critical infrastructure; and

(4) testing and compliance assistance for small entities subject to this Act.

(b) **PRIORITIES.**—Awards shall be prioritized on reasoned, independently reviewed evidence, with uncertainty stated, of severity, exposure, exploitability, dependence of critical services, urgency, additional defensive value, feasible milestones, and proportionate cost. Controlled tests shall be distinguished from field incidents and from projections. Undocumented exposure shall not be treated as zero exposure. Where credible high-consequence exposure is undermeasured, the program may make bounded awards for discovery and validation. Applicant size neither confers priority nor bars an eligible applicant.

(c) **CONFLICTS AND ADDITIONALITY.**—Each award shall have an independent conflicts review and a record of additionality and cost. No award shall be made merely to shift ordinary private compliance costs. An award may fund incremental work related to required remediation only where it provides a distinct, additional public defensive value, with cost allocation, conflicts review, milestones, and no duplicate reimbursement.

(d) **NO PURCHASED TREATMENT.**—No award may be conditioned on, or confer, favorable treatment in any assessment or enforcement matter.

SEC. 803. AWARDS AND VALIDATION.

(a) **CONTENTS.**—Each award shall state the problem, the implementer, milestones, the validation method, security and data limits, and a bounded funding period.

(b) **URGENT AWARDS.**—An urgent award requires a written finding of necessity, a conflicts check, and prompt notice to the Inspector General of the Department of Homeland Security, and is subject to all applicable grant and fiscal laws.

(c) **VALIDATION.**—The claimed result of each award shall be verified reproducibly where feasible, and residual risk shall be reported. A count of patches is not proof of effectiveness in the field.

(d) **CLAWBACK.**—Funds may be recovered for misuse, after notice, an opportunity to respond, and review under the procedures applicable to the award.

SEC. 804. ACCOUNTABILITY.

The Director of the Cybersecurity and Infrastructure Security Agency shall publish annually minimized totals and recipients, milestones met and missed, validated outcomes, limitations, and burden, withholding live exploit details and personal data only as necessary. Acceptance of an award does not release any person from liability for negligence, concealment, or other underlying responsibility, and does not relieve a recipient of any duty to remediate.

SEC. 805. LIMITS.

Nothing in this title creates a central repository of model weights or conversations, or any offensive cyber, surveillance, law enforcement, or diplomatic authority, and nothing in this title provides for the payment of losses generally or for catastrophic insurance.

TITLE IX—ENFORCEMENT, REMEDIES, AND JUDICIAL REVIEW**SEC. 901. CIVIL PENALTIES.**

(a) **LIABILITY.**—A person that violates a provision of title II or title VII, a compelled restriction, or a rule or order issued under title II or title VII, shall be liable to the United States for a civil penalty in an amount determined under subsection (b). A person is liable only with the culpability required by the provision violated or, where the provision specifies no state of mind, only if the person knew or reasonably should have known the facts constituting the violation. This section does not apply to title III, which is enforced under section 305, or to an order of the Federal Trade Commission under section 704(e), which is enforced under section 5(l) of the Federal Trade Commission Act (15 U.S.C. 45(l)).

(b) **AMOUNTS.**—

(1) **TIER 1.**—For a violation of a recordkeeping, notification, or registration requirement, not more than \$100,000 for each violation.

(2) **TIER 2.**—For a violation of section 202, 203, 204, 205, 207, or 211(b), of title VII, or of an order under section 205(f) or of an order of the Administrator under section 704(e), other than a violation described in paragraph (1), not more than \$1,000,000 for each violation.

(3) **TIER 3.**—For a knowing and material violation of a compelled restriction that is lawful and in effect, of which the person had legally sufficient notice, or a knowing and material false statement or omission in a safety case, certification, report, framework, or deployment summary under this Act, not more than \$10,000,000 for each violation.

(4) CONTINUING VIOLATIONS.—Each day on which a violation continues is a separate violation.

(5) AGGREGATE LIMIT.—The total of civil penalties under paragraphs (1) and (2) for violations arising from a single related course of conduct shall not exceed \$50,000,000. This paragraph does not limit penalties under paragraph (3).

(c) FACTORS.—In determining the amount of a penalty, the court shall consider the nature, circumstances, extent, and gravity of the violation; the culpability of the violator; any history of violations; the violator's size and ability to pay; good-faith efforts to comply and to self-report; and the harm caused or risked.

(d) ASSESSMENT BY COURT.—A civil penalty under this section may be assessed only by a district court of the United States in a civil action brought by the Attorney General, or by the Administrator under section 902(c). Any party shall be entitled to trial by jury on any issue triable of right by jury.

(e) LIMITATIONS.—An action for a civil penalty under this section shall be commenced not later than 5 years after the date on which the violation occurred, or, for a violation that was concealed, 5 years after the date on which the Administrator discovered or reasonably should have discovered it.

(f) NO NEW CRIME.—This Act creates no new criminal offense. Existing criminal law, and the power of a court to punish contempt of its lawful orders under section 401 of title 18, United States Code, are unaffected and remain subject to their own predicates and procedures.

SEC. 902. ENFORCEMENT BY THE ADMINISTRATOR.

(a) CIVIL ACTIONS.—The Administrator may bring a civil action in a district court of the United States to enforce a direction under section 202(b)(7), an evidence demand under section 205(e), an order under section 205(f), an order of the Administrator under title VII, or any other duty under title II.

(b) PROCESS.—In each enforcement proceeding, the person against whom enforcement is sought shall receive notice, a usable basis for the claim (including under section 905 where protected information is involved), an opportunity to contest, a reasoned decision, and all ordinary defenses.

(c) LITIGATION AUTHORITY.—The Administrator may bring actions under this section and section 901 through attorneys of the Administration if the Attorney General, after notice, does not commence the action within 45 days.

(d) **REPORTING VIOLATIONS.**—A violation of section 204 requires, for a violation described in section 204(f)(5), the materiality and culpability specified in section 204(f)(5), or, for a violation described in section 204(j)(1), the elements of the applicable subparagraph of section 204(j)(1) and materiality under section 204(j)(3). Truthful preliminary uncertainty, or an inability to produce records that do not exist, is not by itself a violation.

SEC. 903. REVIEW OF FINAL ACTIONS.

(a) **PETITION FOR REVIEW.**—A person aggrieved by a final rule, determination, designation, condition, order, or other final action of the Administrator under this Act, other than a compelled restriction under section 206 or a matter for which section 202(c)(9) provides the route of review, may obtain review by filing a petition for review in the United States Court of Appeals for the District of Columbia Circuit, or for the circuit in which the person resides or has its principal place of business, not later than 60 days after the action is published in the Federal Register or, for an action directed to a particular person, served on that person.

(b) **JURISDICTION.**—On the filing of the petition, the court has jurisdiction, which becomes exclusive on the filing of the record, to affirm, modify, or set aside the action in whole or in part.

(c) **STANDARD OF REVIEW.**—The court shall decide questions of law independently. Findings of fact made on the record of a proceeding that provided notice and an opportunity to respond are conclusive if supported by substantial evidence on the record as a whole. Otherwise, the court shall apply section 706 of title 5, United States Code.

(d) **REVIEWABLE ISSUES.**—Issues reviewable under this section include scope, the competence and conflicts of an assessor, privilege, a designation of control, a condition, an extension of time, and the timestamps of any period under this Act. An issue described in this subsection may be raised on review of the final action to which it relates, and subsection (g) does not bar raising it in an enforcement proceeding if review of that final action was not available.

(e) **STAYS AND PROTECTION.**—Filing a petition does not stay the action. The court may narrow a demand or order, issue protective orders, and grant a stay where warranted.

(f) **EXPEDITION.**—It shall be the duty of the court to advance on the docket and to expedite to the greatest possible extent the disposition of a petition under this section that challenges a designation under section 201(b), an action under section 202(b), a condition under section 203(d), an evidence demand under section 205(e), an order under section 205(f), a determination under section 204(b)(5)(B), or an action under section 210.

(g) **PRECLUSION.**—An action of the Administrator for which review could have been obtained under this section shall not be subject to judicial review in a civil proceeding for enforcement, except where the person lacked notice of the action or standing to seek review under this section, where the defense rests on evidence that first arose, first became lawfully available, or could not reasonably have been discovered by the person with reasonable diligence before the period for review ended, or where timely and effective review was otherwise not actually available. This subsection does not permit a person that deliberately bypassed review that was genuinely available to obtain review in an enforcement proceeding.

SEC. 904. EMERGENCY RESTRAINT PROCEEDINGS.

Proceedings concerning a compelled restriction are governed by section 206. No notice or exhaustion requirement bars an immediate challenge under section 206(d). Lawful judicial powers, standing, and remedies otherwise available are preserved.

SEC. 905. PROTECTED INFORMATION IN CIVIL PROCEEDINGS.

(a) **SCOPE.**—This section applies to any proceeding under this Act, and to review under section 504, in which the United States relies on, or a party seeks, classified information, sensitive security information, privileged law enforcement information, or information whose disclosure the court finds would reveal an unmitigated exploitable vulnerability (in this section referred to as "protected information").

(b) **RECORD.**—The court shall receive the complete preserved record, subject to rulings on lawful privilege. Parties shall receive relevant material that can lawfully be disclosed, under protective order.

(c) **SUBSTITUTES.**—

(1) **PROPOSAL.**—For protected information that the United States seeks to withhold, the United States shall document the security need and propose a usable nonclassified basis and a substitute, which may be a redaction, a summary, a statement admitting relevant facts, or disclosure to a special advocate or to cleared counsel.

(2) **ADEQUACY.**—The court shall determine whether the substitute will provide the affected party with substantially the same ability to contest the relevant issue as disclosure of the protected information would. The Administrator may not both select a substitute and certify its adequacy.

(3) **CONSEQUENCES.**—If the court finds that an adequate contest on a necessary point is impossible within the controlling period, the court may refuse to rely on the

information, narrow the relief, or deny the relief sought, and in a proceeding under section 206 shall deny continuation. Inspection by the court alone to test a protection or substitute is not adversarial review of the merits.

(d) SPECIAL ADVOCATES.—

(1) PANEL.—Not later than 180 days after the date of enactment of this Act, the chief judge of the United States District Court for the District of Columbia shall designate a panel of not fewer than 5 attorneys eligible to serve as special advocates, who possess expertise in artificial intelligence, computer security, national security law, or civil liberties, and who are eligible for access to classified information. The chief judge shall maintain rules on conflicts, rotation, and technical competence. Until the panel is designated, and whenever no panel member is available, the court may appoint as a special advocate any attorney who meets the requirements of this paragraph. The absence of a special advocate extends no period under section 206.

(2) CLEARANCE.—The Director of National Intelligence shall seek to complete the adjudication of a security clearance for an attorney designated to the panel not later than 30 days after designation, and shall report to the court and to the committees of jurisdiction each adjudication not completed within that period.

(3) APPOINTMENT.—The court shall appoint a special advocate from the panel in each proceeding described in section 206(f)(1), and may appoint one in any other proceeding under this section.

(4) ACCESS.—A special advocate shall have access to all protected information relied on by the United States and to any other material the court determines is relevant, and may have access to classified information only if eligible for such access and to the extent consistent with the national security of the United States. If a special advocate is denied access to protected information relied on by the United States, the United States may not rely on that information in the proceeding, and section 206(f)(5) applies.

(5) COMPENSATION.—A special advocate shall be compensated by the court at a rate the court considers appropriate, from funds appropriated to the judiciary.

(e) PROCEDURES.—The Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence, shall prescribe security procedures for proceedings under this section not later than 180 days after the date of enactment of this Act.

(f) CONSTRUCTION.—The Classified Information Procedures Act (18 U.S.C. App.) does not apply to proceedings under this section, except as the court may adopt its procedures consistent with this section.

SEC. 906. ACTIONS TO COMPEL DISCRETE DUTIES.

(a) **IN GENERAL.**—A person with standing may bring a civil action in the United States District Court for the District of Columbia to compel the Administrator to perform a discrete, nondiscretionary duty under this Act that has not been performed by its deadline, including a disposition under section 206(i), the issuance of a rule under section 201(d), a publication under section 106 or 206(g), or a provisional determination under section 210(c)(2).

(b) **NOTICE.**—The action may be brought only after 10 days' written notice to the Administrator, except that no notice is required where the plaintiff shows a risk of urgent irreparable harm.

(c) **RELIEF.**—The court may order performance of the duty and grant declaratory relief, but may not direct the substance of a discretionary decision and may not award damages against the United States. The court may award costs of litigation, including reasonable attorney's fees, to a substantially prevailing plaintiff.

(d) **LIMITATION.**—An action under this section shall be brought not later than 1 year after the later of the deadline for the duty and the date on which the plaintiff knew or reasonably should have known of the failure to perform it. While a failure to perform a duty that remains required continues, an action to compel future performance may be brought at any time.

(e) **SECTION 206.**—No notice or exhaustion requirement under this section delays an immediate challenge under section 206(d).

SEC. 907. EXISTING RIGHTS AND SAFEGUARDS.

(a) **NO IMMUNITY.**—Passing an assessment, complying with a protocol, receiving an award under title VIII, or making a good-faith report does not immunize underlying unlawful conduct.

(b) **EXISTING CLAIMS.**—Nothing in this Act creates a private right of action except as provided in sections 209, 305(c), and 906, or limits any claim, remedy, or defense available under other Federal or State law.

(c) **NO FINDING OF ADEQUACY.**—The absence from this Act of any other private right of action, or of any duty on deployers, is not a finding that existing remedies or duties are adequate.

SEC. 908. STUDIES.

(a) **DEPLOYMENT GAP INVENTORY.**—Not later than 1 year after the date of enactment of this Act, the Administrator, in consultation with the heads of the relevant Sector Risk Management Agencies, the Secretary of Health and Human Services, the Secretary of Labor, the Equal Employment Opportunity Commission, the Consumer Financial Protection Bureau, and the Federal Trade Commission, shall submit to Congress an inventory of the Federal duties that apply to the deployment of artificial intelligence systems in health care, employment, financial services, and critical infrastructure, identifying for each duty its actor, predicate, recipient, and remedy, and each gap, with legislative recommendations.

(b) **INSURANCE AND COMPENSATION.**—Not later than 2 years after the date of enactment of this Act, the Comptroller General shall submit to Congress a study of the availability of insurance for harms from artificial intelligence systems, the compensation of persons injured by such harms, and options for Federal action, including financial-assurance requirements, compensation mechanisms, and a private right of action, with the actors, injuries, causation standards, remedies, and fiscal effects of each option.

(c) **ACT REVIEW.**—Not later than 2 years after the date of enactment of this Act, and every 3 years thereafter, the Comptroller General shall submit to Congress a review of the implementation of this Act, including the workload, backlog, timeliness, and cost of each deadline and procedure, reversals on review, missed incidents, privacy and security failures, validated outcomes, the supply, independence, conflicts, and quality of accredited assessors, each shortage determination under section 207(c)(3), and the implementation of section 211, with recommendations.

(d) **EXISTING-AUTHORITY RESPONSE PLAN.**—Not later than 180 days after the date of enactment of this Act, the Administrator, in consultation with the agencies described in subsection (a), the Attorney General, the Federal Communications Commission, and other agencies with relevant existing authority, shall publish a task-specific plan for testing and responding to documented artificial-intelligence harms involving fraud and impersonation, nonconsensual intimate imagery and sexual exploitation, discriminatory decisions, and unsafe consequential deployment. For each harm, the plan shall identify the responsible agency, existing legal predicate, affected actors, evidence and technical testing needed, complaint and referral route, available remedy, resources legally available for the task, and an accountable implementation schedule. Each participating agency shall identify and implement feasible steps within its existing authority and available appropriations, and shall state any unresolved gap requiring legislation. The plan shall preserve existing rights and earlier reporting duties, protect personal data, and report progress annually. This subsection confers no new sector enforcement authority on the Administration and no authority to waive an existing duty or remedy; a plan or

study is not a finding that existing protection is adequate.

TITLE X—FUNDING, TRANSITION, AND EFFECTIVE DATES

SEC. 1001. AUTHORIZATION OF APPROPRIATIONS.

(a) **ADMINISTRATION OPERATIONS.**—There is authorized to be appropriated to the Administration for operations, including evaluation, incident intake, inspection, security, legal and privacy functions, the Office of Incident Review, the Office of Inspector General, and the assessor program, \$150,000,000 for fiscal year 2027, \$200,000,000 for fiscal year 2028, and \$230,000,000 for each of fiscal years 2029 through 2031.

(b) **ESTABLISHMENT.**—There is authorized to be appropriated to the Administration \$106,000,000 for fiscal year 2027 for one-time costs of establishment, including secure facilities and computing, to remain available until expended.

(c) **RESILIENCE PROGRAM.**—There is authorized to be appropriated to the Cybersecurity and Infrastructure Security Agency to carry out title VIII \$150,000,000 for each of fiscal years 2027 through 2031, of which not more than 8 percent may be used for administration.

(d) **SMALL ENTITY SUPPORT.**—There is authorized to be appropriated to the Administration \$30,000,000 for each of fiscal years 2027 through 2031 for testing and compliance assistance, including vouchers for accredited assessments, for small entities subject to this Act.

(e) **FEDERAL TRADE COMMISSION.**—There is authorized to be appropriated to the Federal Trade Commission \$6,500,000 for each of fiscal years 2027 through 2031 to carry out title III.

(f) **JUDICIARY.**—There is authorized to be appropriated to the judiciary \$6,000,000 for each of fiscal years 2027 through 2031 for proceedings under sections 206 and 905, including compensation of special advocates.

(g) **SEPARATE ACCOUNTS.**—Amounts for operations, establishment, and programs shall be maintained in separate accounts.

(h) **NO CAPACITY FINDING.**—An authorization or appropriation under this section is not a finding that the Administration has the capacity required by section 210(b).

SEC. 1002. FEES.

(a) **AUTHORITY.**—The Administrator may assess and collect fees from covered developers, based on risk and scale, and from operators subject to section 303(c)(1), to supplement appropriations for assessments under sections 202, 203, and 303(c) and for the pooled payment of accredited assessors.

(b) **LIMITS.**—Total fees collected in a fiscal year shall not exceed 25 percent of the amount appropriated for that year under section 1001(a). Fees shall supplement, and not replace, appropriations.

(c) **AVAILABILITY.**—Fees shall be deposited and credited as offsetting collections to the Administration's operations account, shall be available only to the extent and in the amounts provided in advance in appropriations Acts, and shall remain available until expended.

(d) **NO PURCHASED TREATMENT.**—Payment of a fee confers no priority, favorable result, or choice of assessor. Assignment of an assessor shall not depend on the assessed person's selection or control of payment to the assessor.

(e) **RULE.**—The Administrator shall establish fees by rule after notice and comment, and shall publish annually the fees collected and their use.

SEC. 1003. TRANSITION.

(a) **PLAN.**—The transition plan under section 104(c) shall also identify the Administration's acting officials, the use of the personnel authorities under section 103, and the arrangements for the independence of the Office of Incident Review.

(b) **CAPACITY TARGETS.**—The Administrator shall publish targets for building and retaining capacity and shall report progress against them in the annual report under section 106(f). Targets are planning and reporting duties and do not guarantee any level of capacity.

SEC. 1004. EFFECTIVE DATES AND INTERIM REPORTING.

(a) **ON ENACTMENT.**—Except as otherwise provided in this section, this Act takes effect on the date of enactment, including the duties to appoint officers, to plan, and to issue rules.

(b) **INTERIM REPORTING.**—

(1) **EFFECTIVE DATE.**—Sections 204 and 304 take effect 90 days after the date of enactment of this Act.

(2) **RECEIVER.**—The Administrator, or an acting Administrator serving under subchapter III of chapter 33 of title 5, United States Code, is the receiver of reports under

those sections. Until the Administrator publishes in the Federal Register notice that the intake of the Administration is operative, and at any later time when that intake is not operative, the Director of the National Institute of Standards and Technology, acting through the Center for AI Standards and Innovation or any successor organization, shall be the continuity receiver, with authority limited to the secure intake, acknowledgment, preservation, protection, triage, and task-specific lawful referral of reports under section 204(e), and the reasoned disposition required by section 204(i) within the period that section provides, and no other authority under this Act. The Director shall designate by name the officer responsible for these functions. Receipt confers no emergency authority, sector enforcement authority, or other authority of the Administrator.

(3) ROUTING RECIPIENTS.—For the purposes of reports routed under this Act, the Cybersecurity and Infrastructure Security Agency, the Assistant Secretary for Preparedness and Response of the Department of Health and Human Services, and the Federal Trade Commission each have authority to receive, preserve, and act on routed reports within their existing authorities, for the purposes of the routing only.

(4) FUNDING OF CONTINUITY.—Amounts made available to the National Institute of Standards and Technology for the Center for AI Standards and Innovation, or any successor organization, may be used to carry out paragraph (2), and the Administrator may transfer to that Institute, for that purpose, amounts appropriated under section 1001(a).

(5) SAFEGUARDS.—Each receiver and recipient shall maintain minimized routing, protected tamper-evident records and preservation of gaps, secure submission and acknowledgment, tested escalation, whistleblower safeguards, and reasoned disposition.

(6) PUBLICATION.—Not later than 45 days before the date described in paragraph (1), the Director of the National Institute of Standards and Technology shall establish and test the channel and a safe alternate, and shall publish the responsible channel, the statutory definitions, instructions for notice, and the safe alternate procedure.

(c) INTERIM GUIDANCE.—Interim guidance may explain the statutory actors, predicates, and duties, but may not enlarge them. Existing reporting laws keep their own recipients, predicates, and deadlines.

(d) LATER DATES.—

(1) CONTAINMENT AND SECURITY.—Section 205(a), (b), (c), and (e)(2) take effect 180 days after the date of enactment of this Act.

(2) **COVERAGE AND TESTING.**—Sections 202 and 203 take effect 1 year after the date of enactment of this Act. A failure to issue a rule under section 201(d) by that date is enforceable under section 906. Section 201(a)(4) takes effect 90 days after the date of enactment of this Act, and until the Administrator prescribes a form, a notice under that section may be given by any written means that identifies the person, the run, and the estimated computing power.

(3) **TITLE III.**—Sections 302 and 303 take effect 1 year after the date of enactment of this Act.

(4) **TITLE V.**—Title V applies to covered actions taken on or after the date of enactment of this Act.

(5) **STATE LAW.**—Section 210(a) has no effect until a determination under section 210(b) is in effect, and then only to the extent of that determination.

(e) **NO CAPACITY WAIVER.**—No effective date under this section depends on a declaration by the Administration that it is ready, and there is no general waiver of any duty for lack of capacity. Existing duties and review are preserved during the transition. New standards create no retrospective liability.

SEC. 1005. CONTINUITY DURING A LAPSE IN APPROPRIATIONS.

(a) **PLANS.**—The Administrator shall maintain lawful plans for continuity of acting authority, purpose-limited secure intake, and a contingency for a lapse in appropriations consistent with section 1342 of title 31, United States Code. This section does not authorize the obligation or expenditure of funds that are not available.

(b) **DUTIES CONTINUE.**—The expiration of an authorization of appropriations under this Act does not repeal or suspend any duty under this Act. The continuation of a duty does not supply funds.

SEC. 1006. RULES OF CONSTRUCTION.

(a) **NO GUARANTEE.**—Nothing in this Act guarantees the prevention of any harm, the cooperation of any foreign government, or the uninterrupted operation of any system.

(b) **OTHER AUTHORITY.**—Except as expressly provided, nothing in this Act limits or expands the authority of any Federal agency under any other provision of law.

(c) **SPEECH.**—Nothing in this Act authorizes the Administrator to regulate the lawful viewpoint of any person or of the lawful outputs of any system.

SEC. 1007. SEVERABILITY.

(a) **IN GENERAL.**—Except as provided in subsection (b), if any provision of this Act, or its application to any person or circumstance, is held invalid, the remainder of this Act and its application to other persons or circumstances shall not be affected.

(b) **SAFEGUARDS INSEPARABLE FROM POWERS.**—The authority to impose or continue a compelled restriction under section 206 is inseparable, for the affected application, from the substantive predicates, Government burdens, meaningful protected adversarial hearing and decision, self-executing lapse, court-only continuation limits, and prohibitions on tolling and reset required by that section. A holding of invalidity may not be used to preserve or enlarge that authority by removing a required safeguard; the restriction authority is unavailable to the extent that the affected application cannot satisfy every such safeguard. Section 210(a) is likewise inseparable from the conditions and gap protections in section 210(b) and (c). A holding of invalidity affecting a required condition does not authorize displacement of the affected State obligation without that condition. Independently applicable statutory duties and lawful powers of other agencies retain their own predicates and safeguards.