RIGHT TO RUN

Right to Compute and Access Advanced Intelligence Act of 2027

Federal bill · Version 1 · September 2026 · Three titles, 38 sections

Proposed for the 120th Congress. Not introduced.

DISCUSSION DRAFT — V1

120TH CONGRESS — 1ST SESSION

H. R. ______

To protect the right of the people to acquire and use computational resources; to protect lawful access to, possession of, sharing of, and independent operation of advanced artificial intelligence, including for personal defense, safety, and resilience; to prohibit direct and indirect capability-based restrictions by government; to require risk management policies for critical infrastructure controlled by artificial intelligence; to provide remedies against Federal and State actors; to establish a measurable public-access program for advanced civilian artificial intelligence; and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

____________________, 2027

Mr./Ms. ________________ (for himself/herself and Mr./Ms. ________________) introduced the following bill; which was referred to the Committee on ________________, and in addition to such other committees as the Speaker may determine, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.

A BILL

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 "Right to Compute and Access Advanced Intelligence Act of 2027".

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

SEC. 2. FINDINGS.

Congress finds the following:

(1) Computational resources and artificial intelligence are instruments of speech, inquiry, commerce, education, scientific research, cybersecurity, emergency preparedness, personal safety, and the defense of persons, property, communications, and infrastructure.

(2) The proper subject of governmental regulation is conduct. A person who commits fraud, intrusion, theft, or violence may be prosecuted for that conduct whether or not an artificial intelligence system assisted it. The capability of a lawfully possessed tool is not itself a harm, and the possibility that a capability could be misused by someone is not a lawful basis for denying it to everyone.

(3) A standard that permits government to restrict capability whenever it can articulate a sufficiently weighty interest concedes the question this Act is meant to settle. Accordingly, this Act does not subject capability-based restrictions to balancing. It withholds the authority to impose them.

(4) Governments have proposed or adopted restrictions on artificial intelligence that turn on the capability of a system rather than on unlawful conduct, including the training-compute reporting threshold in Executive Order 14110 (October 30, 2023; revoked January 20, 2025); the controls on artificial-intelligence model weights in the January 2025 Framework for Artificial Intelligence Diffusion, which the Department of Commerce announced on May 13, 2025, it would not enforce and intended to rescind, but which had not been formally rescinded and remained in the Code of Federal Regulations as of May 2026, the Comptroller General having determined on May 12, 2026, in decision B-337935, that the non-enforcement announcement was itself a rule that had not been submitted to Congress as chapter 8 of title 5, United States Code, requires; and the compute-keyed obligations in California's Transparency in Frontier Artificial Intelligence Act (2025) and New York's Responsible AI Safety and Education Act (2025), as amended in 2026 and effective January 1, 2027.

(5) Restrictions keyed to capability, compute, parameter count, or benchmark score do not distinguish lawful from unlawful use and tend to reserve the most capable tools to government and to large institutions while denying substantially comparable tools to individuals, small businesses, researchers, and local governments.

(6) Government can restrict access indirectly, through pressure on cloud providers, hardware suppliers, payment processors, and other intermediaries, as readily as directly. In *National Rifle Association of America v. Vullo*, 602 U.S. 175 (2024), the Supreme Court held that a government official may not coerce a private party to punish or suppress protected speech on the government's behalf.

(7) Source code is expressive, and restrictions on its creation and distribution implicate the First Amendment. In *Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000), the court of appeals held that computer source code is protected by the First Amendment because it is an expressive means for the exchange of information and ideas. In *Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001), the court of appeals likewise treated code as protected speech, while sustaining a restriction directed at the functional operation of the code rather than at its expressive content. Congress finds that the creation, publication, and receipt of model weights is expressive and scientific activity of the same character.

(8) The Supreme Court recognized in *District of Columbia v. Heller*, 554 U.S. 570 (2008), that individual self-defense is a core interest of the people. Advanced artificial intelligence is increasingly the means by which individuals protect their lives, homes, property, communications, networks, and

infrastructure from physical, digital, and environmental threats. Congress protects that defensive use by statute under its powers to regulate interstate commerce and to make all laws necessary and proper thereto, without characterizing software or computational resources as arms.

(9) Montana enacted the first Right to Compute Act in 2025 (Chapter 150, Laws of Montana 2025) with bipartisan support, pairing a general protection for computational resources with a risk-management requirement for critical infrastructure controlled by artificial intelligence. Other States have introduced or advanced similar measures.

(10) INTERSTATE CHARACTER OF ADVANCED ARTIFICIAL INTELLIGENCE.—

(A) The acquisition, provision, and use of computational resources and artificial intelligence systems are economic activities conducted in and substantially affecting interstate commerce. Compute capacity, model weights, inference services, and the hardware on which they depend are bought, sold, leased, and transferred across State lines as a routine matter of commerce.

(B) Advanced artificial intelligence systems are typically trained in one State or several, hosted in data centers in others, and delivered to users in every State through networks that do not correspond to State boundaries. A user's request is routinely served by infrastructure in a State the user has never entered.

(C) Providers of advanced artificial intelligence generally cannot partition service by State at reasonable cost. A capability-based restriction imposed by a single State therefore operates in practice as a restriction on the national market, because a provider's compliance choice is to degrade the product everywhere or to exit that State.

(D) Divergent State capability-based restrictions, in the aggregate, impose compliance costs and design constraints on an interstate market, deter entry by smaller developers who cannot absorb multi-jurisdiction compliance, and reduce the capabilities available to users in States that have imposed no restriction at all.

(E) Congress therefore finds that a uniform national rule prohibiting governmental capability-based restrictions is necessary to protect interstate commerce in computational resources and artificial intelligence systems from substantial burden and fragmentation.

(11) FEDERAL PREEMPTION ACTIVITY.— Executive Order 14365 (December 11, 2025) directed the Attorney General to establish a litigation task force to challenge State artificial-intelligence laws, directed the Federal Communications Commission and the Federal Trade Commission to develop preemption standards, conditioned certain Federal funds on State regulatory practice, and directed the preparation of proposed legislation establishing a Federal policy framework preempting State artificial-intelligence laws. That order rests on executive action rather than an Act of Congress. This Act addresses the same subject by statute, preempts State law only as expressly provided in section 115, and reaches capability-based restrictions without displacing State regulation of conduct.

(12) STATE PROTECTIVE LEGISLATION.— Several States have enacted or advanced legislation protecting the right to acquire and use computational resources. Nothing in this Act is intended to

displace such legislation, and the preemption provided by this Act is limited to State and local measures that impose capability-based restrictions on an interstate market.

(13) This Act does not alter the siting, energy use, water use, or generally applicable taxation of data centers and other physical facilities, which remain governed by other law. A tax or fee imposed by reference to the capability of an artificial intelligence system, or to training or inference compute, is a capability-based restriction governed by this Act rather than a generally applicable facility tax. This Act does not limit lawful export controls, sanctions, or the protection of classified information.

SEC. 3. DEFINITIONS.

In this Act:

(1) ACCESS.— The term "access" means the practical ability to obtain and lawfully use an artificial intelligence system or its capabilities through local execution, remote inference, an application programming interface, a commercial or public service, cloud computing, open-weight distribution, distributed computing, or another technological means.

(2) ADVANCED ARTIFICIAL INTELLIGENCE.— The term "advanced artificial intelligence" means an artificial intelligence system exhibiting capabilities at or near the leading edge of demonstrated, nonclassified civilian artificial intelligence capabilities deployed, used, or made available to government, commercial, academic, nonprofit, or other institutional users, regardless of whether equivalent public access is then available.

(3) ARTIFICIAL INTELLIGENCE SYSTEM.— The term "artificial intelligence system" means a machine-based system that, for explicit or implicit objectives, infers from inputs how to generate outputs, including predictions, content, recommendations, decisions, plans, code, analyses, or actions, that can influence physical or virtual environments.

(4) CAPABILITY-BASED RESTRICTION.— The term "capability-based restriction" means a governmental restriction, whether legal or practical, that limits a covered person’s ability to acquire, possess, develop, train, publish, share, operate, or access an artificial intelligence system or computational resource because of, or by reference to, the capability of that system or resource, including its intelligence, scale, autonomy, reasoning ability, knowledge, cybersecurity ability, scientific or technical ability, context capacity, tool use, sustained-operation capacity, training or inference compute, parameter count, benchmark performance, architecture, openness or modifiability, or potential for misuse. The term includes such a restriction whether or not it is expressed as a threshold, and whether imposed directly or through a technical proxy or other indirect means described in section 105(c).

(5) COMPUTATIONAL RESOURCE.— The term "computational resource" includes hardware, software, processors, accelerators, storage, networks, data-center capacity, algorithms, artificial intelligence systems, model weights, and other resources used to perform computation.

(6) COVERED INTERMEDIARY.— The term "covered intermediary" includes a cloud or hosting provider, chip or hardware supplier, model distributor, application store, payment processor,

financial institution, internet or telecommunications provider, data-center operator, government contractor, or other person positioned to enable, deny, condition, or materially burden access to computational resources or artificial intelligence.

(7) COVERED PERSON.— The term "covered person" means a citizen or national of the United States, a lawful permanent resident, an individual otherwise lawfully present in the United States, or an entity organized under the laws of the United States or of a State, except as otherwise expressly provided by Federal law.

(8) CRITICAL INFRASTRUCTURE.— The term "critical infrastructure" has the meaning given that term in section 1016(e) of the Critical Infrastructures Protection Act of 2001 (42 U.S.C. 5195c(e)).

(9) DEFENSIVE USE.— The term "defensive use" means lawful use of a computational resource or artificial intelligence system to protect the life, safety, home, property, communications, data, networks, systems, or infrastructure of the user or of a person the user is authorized to protect, including detection, prevention, mitigation, response, and recovery.

(10) GOVERNMENT ENTITY.— The term "government entity" means the Federal Government, a State, a political subdivision of a State, and any agency, officer, employee, or agent of any of them acting in an official capacity.

(11) MEANINGFUL PUBLIC ACCESS.— The term "meaningful public access" means access that is practically usable by members of the public and is not rendered illusory by prohibitive price, artificial scarcity, unreasonable identity or institutional-status requirements, excessive delay, materially inadequate context or tool access, unusable rate limits, or insufficient sustained-operation capacity.

(12) MODEL WEIGHTS.— The term "model weights" means numerical or computational parameters learned, generated, or otherwise established during development or training of an artificial intelligence system and used by the system to produce outputs.

(13) SPECIALLY PRIVILEGED INSTITUTION.— The term "specially privileged institution" means a private person permitted by a government entity to possess, operate, or access a capability under a license, exemption, contract, grant, registration, or other governmental authorization that is not made available on neutral terms to the public.

(14) SUBSTANTIAL BURDEN.— The term "substantial burden", with respect to a right protected by title I, means a governmental measure that prohibits, or that in practical operation materially impairs, the exercise of that right. The term includes a prohibition, a capability-based license, an excessive or discriminatory fee or tax, an unnecessary registration requirement, an unreasonable delay or waiting period, an institutional-eligibility or credentialing requirement, an excessive identity-verification requirement, and the provision of access that is materially degraded by artificial scarcity, unusable rate limits, materially inadequate context capacity or tool access, insufficient sustained-operation capacity, or restriction to an obsolete or materially less capable version. Nominal availability that ordinary users cannot practically use is a substantial burden.

(15) SUBSTANTIALLY COMPARABLE.— The term "substantially comparable", with respect to two artificial intelligence capabilities, means that the capabilities perform at materially similar levels

across useful task performance, reasoning, planning, coding, scientific and technical work, cybersecurity, multimodal capability, context capacity, tool use, sustained operation, reliability, latency, availability, rate limits, and cost, considered together and without treating any single benchmark, parameter count, compute threshold, or architecture as dispositive. Where a framework established under section 205(a) is in effect, the measures adopted under section 205(c) shall be used. This paragraph applies whether or not title II is in effect. A difference in price, interface, branding, rate limit, or terms of service does not by itself make a capability not substantially comparable. The government entity bears the burden of demonstrating that a capability it possesses is not substantially comparable to one it restricts.

(16) STATE.— The term "State" means each of the several States, the District of Columbia, and each territory or possession of the United States.

(17) TECHNICAL PROXY.— The term "technical proxy" means a measure, including parameter count, training or inference compute, hardware quantity, memory, training cost, benchmark score, context length, autonomy, agentic operation, tool use, multimodality, architecture, openness, modifiability, code-generation ability, cybersecurity capability, scientific capability, or any substantially equivalent criterion, used to identify or restrict a system because of its capability rather than because of a specific unlawful use. The term includes any measure, however labeled, the purpose or practical effect of which is to impose a capability-based restriction.

(18) WILLING PROVIDER.— The term "willing provider" means a private or public person that voluntarily offers lawful access to an artificial intelligence system or computational resource, subject to lawful contract terms.

TITLE I—RIGHTS AND REMEDIES

SEC. 101. APPLICABILITY; RULE OF CONSTRUCTION.

(a) GENERAL APPLICATION.— Except as provided in subsection (c), this title applies to all Federal law and to the implementation of Federal law, whether statutory or otherwise and whether adopted before or after the date of enactment of this Act.

(b) LATER-ENACTED LAW.— A Federal statute enacted after the date of enactment of this Act is subject to this title unless that statute explicitly excludes application of this title by specific reference to this section.

(c) ENUMERATED EXCLUSIONS.— This title does not create a right to obtain classified information; compel access to a military, intelligence, or law-enforcement operational system not offered for civilian access; require access by a foreign person prohibited by law; or override a restriction limited to an export, reexport, in-country transfer, sanctions transaction, or foreign end use or end user. A domestic restriction on possession, use, or access by a covered person that extends beyond those subjects remains subject to this title unless Congress expressly provides otherwise under subsection (b).

(d) CAPABILITY ALONE.— Possession of, access to, development of, or use of an otherwise lawful computational or artificial-intelligence capability does not become unlawful solely because the capability is advanced, dual-use, capable of cybersecurity research, capable of generating code, or capable of performing tasks that could also be misused.

(e) STATES.— The application of this title to States and political subdivisions is as follows.

(1) DUTIES.— Sections 103(d), 104(b), 104(c), 105, 106, 107, 108, 110(e), 112(c), 113(e), 116, 118, 119, 121, and 122(c) impose duties on States and political subdivisions.

(2) ENFORCEMENT AND PREEMPTION.— Sections 114 and 115 govern the enforcement of this title against, and its preemptive effect on, States and political subdivisions.

(3) FEDERAL GOVERNMENT ONLY.— Sections 117 and 120 impose duties on the Federal Government only, and no State or local officer is liable under this title for conduct described in either section.

(4) EXCLUSIVE STATEMENT.— This subsection is the exclusive statement of the provisions of this title that impose duties on a State or political subdivision, and a reference elsewhere in this title to a government entity is to be read accordingly.

SEC. 102. RIGHT TO COMPUTE, DEVELOP, AND SHARE.

(a) IN GENERAL.— A covered person has a statutory right, for lawful purposes, to acquire, own, lease, possess, configure, use, and operate computational resources.

(b) DEVELOPMENT.— Protected conduct includes lawful development, training, fine-tuning, testing, evaluation, modification, and creation of artificial intelligence systems and software.

(c) SHARING AND COLLABORATION.— Protected conduct includes lawful publication, distribution, transfer, sharing, collaborative development, and provision of artificial intelligence software, model weights, research, and tools that the person is legally entitled to distribute.

SEC. 103. RIGHT TO ACCESS ADVANCED ARTIFICIAL INTELLIGENCE.

(a) IN GENERAL.— A covered person has a statutory right, for lawful purposes, to seek, obtain, purchase, subscribe to, connect to, and use advanced artificial intelligence made available by a willing provider.

(b) CHANNEL NEUTRALITY.— Subsection (a) applies without regard to whether access occurs through local execution, remote inference, cloud service, application programming interface, commercial service, public infrastructure, open-weight model, distributed system, or another technological method.

(c) SUBSTANTIAL BURDENS.— A substantial burden includes a prohibition, capability-based license, excessive or discriminatory fee, unnecessary registration requirement, unreasonable delay, institutional-eligibility requirement, or other measure that in practical operation materially impairs protected access.

(d) NO INSTITUTIONAL GATEKEEPING.— A government entity may not establish, authorize, or require a system of tiered access under which advanced artificial intelligence is available to institutions, credentialed persons, or approved classes of users on terms materially better than those available to covered persons generally.

SEC. 104. RIGHT TO POSSESS AND INDEPENDENTLY OPERATE ARTIFICIAL INTELLIGENCE.

(a) POSSESSION.— A covered person has a statutory right, for lawful purposes, to acquire, possess, store, copy, and operate artificial intelligence software and model weights that the person is legally entitled to obtain or possess.

(b) LOCAL AND OFFLINE OPERATION.— A government entity may not require that an otherwise lawful artificial intelligence system be accessible only through a remote provider, continuous network connection, government-controlled service, or revocable provider authorization merely because the system is advanced or highly capable.

(c) PRIVATE INFERENCE.— A government entity may not require routine disclosure of private prompts, outputs, locally stored model weights, or locally processed information solely as a condition of lawful private operation, except pursuant to lawful compulsory process directed to a particular investigation or proceeding and consistent with the Constitution.

SEC. 105. PROHIBITION ON CAPABILITY-BASED RESTRICTIONS.

(a) CATEGORICAL PROHIBITION.— A government entity may not prohibit, license, permit, ration, meter, register, condition, delay, suppress, or otherwise materially burden the lawful acquisition, possession, development, training, fine-tuning, evaluation, publication, distribution, sharing, operation, or access by a covered person of an artificial intelligence system or computational resource because of, or by reference to, the capability of that system or resource, including its intelligence, scale, autonomy, reasoning ability, knowledge, cybersecurity ability, scientific or technical ability, context capacity, tool use, sustained-operation capacity, training or inference compute, parameter count, benchmark performance, architecture, openness or modifiability, or potential for misuse. The term capability-based restriction has the meaning given in section 3.

(b) STATE RULE; INTERSTATE ACCESS.— A capability-based restriction imposed by a State or political subdivision on the acquisition, possession, development, sharing, operation, or access in or affecting interstate commerce of an otherwise lawful artificial intelligence system or computational resource by a covered person has no force or effect. A covered person is entitled under this subsection to acquire, possess, develop, share, operate, and access such a system or resource free of any such restriction, and may assert that entitlement under section 114. This subsection expressly preempts any State or local law to the contrary, and is to be construed as a regulation of the interstate market in computational resources and artificial intelligence systems and as conferring a right on covered persons, rather than as a direction to a State legislature respecting the enactment of State law.

(c) NO PROXY EVASION.— A capability-based restriction may not be imposed through a technical proxy, a procurement or funding condition, a reporting or registration requirement, a liability rule keyed to capability, an insurance or bonding requirement, a standards or accreditation body, a condition on a license unrelated to computation, a remote attestation or device integrity requirement, a mandatory telemetry or use-reporting requirement, escrow or deposit of model weights with a government entity or its designee, a government-controlled or government-mandated remote disablement capability, a tax or fee imposed by reference to capability or to training or inference compute, a restriction on the sale or transfer of general-purpose computational hardware to a covered person other than a restriction described in section 101(c), or any other indirect means. A restriction imposed through such means is prohibited by subsection (a) to the same extent as a direct restriction.

(d) HARDWARE.— A government entity may not require registration, licensing, or reporting of general-purpose computational hardware by a covered person because the hardware exceeds a computing-capacity threshold, except as to an export, reexport, or transfer described in section 101(c).

(e) INFRASTRUCTURE REGULATION NOT AFFECTED.— This Act does not limit a law of general application governing the siting, zoning, construction, permitting, energy use, energy rates, water use, water discharge, noise, emissions, grid interconnection, or taxation of a data center, power plant, or other physical facility when that law regulates the facility rather than computation itself. Such a law is not a capability-based restriction.

(f) NOT SUBJECT TO BALANCING.— A capability-based restriction is void. Section 108 does not apply to, and supplies no authority for, such a restriction. No governmental interest, however weighty, and no degree of tailoring, however narrow, validates a capability-based restriction, and a court shall not weigh the asserted benefits of such a restriction against the rights protected by this title.

(g) ASSERTED INTERESTS INSUFFICIENT.— An asserted governmental interest in public safety, national security, catastrophic risk, existential risk, systemic risk, technological risk, international competitive position, potential misuse, or the capabilities of artificial intelligence generally does not, standing alone or in combination, constitute authority to impose a capability-based restriction.

(h) CONDUCT UNAFFECTED.— Nothing in this section limits the authority of a government entity to prohibit, investigate, prosecute, or punish conduct that is independently unlawful, including such conduct committed with the assistance of an artificial intelligence system and including conduct furthering a harm described in section 109. Liability attaches to the conduct and not to the capability employed.

SEC. 106. PROHIBITION ON INDIRECT GOVERNMENT RESTRICTIONS.

(a) ANTI-CIRCUMVENTION.— A government entity may not coerce, threaten, materially pressure, direct, induce, or condition a license, grant, contract, procurement opportunity, regulatory benefit, or other governmental advantage on a covered intermediary taking an action that the government entity could not lawfully require directly under this title.

(b) PRACTICAL EFFECT.— A court shall consider the substance and practical effect of the governmental conduct, including threatened adverse action, repeated or coordinated requests, conditioning of benefits, and whether a reasonable intermediary would understand the communication as carrying governmental consequences.

(c) STANDING OF AFFECTED PERSONS.— A covered person whose access to a computational resource or artificial intelligence system is denied, conditioned, or materially degraded by a covered intermediary as a result of conduct prohibited by subsection (a) has suffered an injury in fact for purposes of section 114, whether or not the intermediary itself objects.

(d) RECORDS.— Each Federal agency shall retain, for not less than five years, each written or recorded communication to a covered intermediary requesting, directing, or encouraging the intermediary to deny, condition, or restrict access to a computational resource or artificial intelligence system. Such records are agency records subject to section 552 of title 5, United States Code, and the exemptions in subsection (b) of that section apply.

(e) PRIVATE CHOICE PRESERVED.— Nothing in this section restricts an intermediary from independently setting lawful terms, declining service, managing capacity, or taking action for bona fide commercial, security, fraud-prevention, or safety reasons not materially induced by conduct prohibited by subsection (a).

(f) LAWFUL GOVERNMENT COMMUNICATION.— This section does not prohibit lawful compulsory process, a court order, communication concerning specific independently unlawful conduct, or a content-neutral procurement requirement, provided the communication is not used to accomplish indirectly a restriction that would violate this title if imposed directly.

(g) NOTICE TO AFFECTED PERSONS.—

(1) IN GENERAL.— A covered intermediary described in paragraph (4) that denies, terminates, or materially degrades a covered person's access to a computational resource or artificial intelligence system, in response in whole or substantial part to a communication from a government entity of the kind described in subsection (a), shall notify that person not later than 30 days after the action, and shall state in the notice that a government entity requested or recommended the action and identify the government entity.

(2) EXCEPTIONS.— Paragraph (1) does not apply where notice is prohibited by statute, by a court order, or by a nondisclosure requirement lawfully issued in connection with a criminal investigation or a national security matter, and does not apply to an action taken for a reason described in subsection (e).

(3) DELAYED NOTICE.— Where notice is prohibited under paragraph (2), the intermediary shall provide the notice required by paragraph (1) not later than 30 days after the prohibition lapses.

(4) APPLICABILITY.— This subsection applies to a covered intermediary that, in the preceding calendar year, had annual United States revenue from the provision of computational resources or artificial intelligence systems exceeding $500,000,000.

(5) ENFORCEMENT.— A violation of this subsection shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)), and the Federal Trade Commission shall enforce it with the same jurisdiction, powers, and duties, including the penalties provided in section 5(m)(1)(A) of that Act (15 U.S.C. 45(m)(1)(A)), as though the applicable provisions of that Act were incorporated into this Act. This subsection does not create a private right of action.

(6) ANNUAL REPORT.— A covered intermediary described in paragraph (4) shall publish annually the aggregate number of communications described in subsection (a) that it received, disaggregated by requesting government entity.

SEC. 107. DEFENSIVE COMPUTING, SELF-PRESERVATION, AND RESILIENCE.

(a) PROTECTED DEFENSIVE USE.— Defensive use of a computational resource or artificial intelligence system is protected conduct under sections 102 through 104. Protected defensive use includes lawful use for personal safety; protection of the home and of persons within it; protection of property; cybersecurity, threat detection, intrusion response, and recovery for systems the person owns or is authorized to protect; communications continuity and encryption; emergency preparedness and response; navigation; disaster recovery; infrastructure diagnostics and repair; analysis of environmental, medical, engineering, or scientific hazards; and other lawful activities relating to safety, autonomy, self-preservation, or resilience.

(b) NO RESTRICTION ON DEFENSIVE CAPABILITY.— A government entity may not restrict a covered person's defensive use on the ground that the capability is equal to or greater than a capability the government entity or a specially privileged institution uses for the same defensive purpose. Such a restriction is a capability-based restriction and is void under section 105.

(c) OFFLINE AND DEGRADED CONDITIONS.— Because defensive use is most needed when networks, providers, or government services are unavailable, a government entity may not condition lawful defensive use on continuous connectivity, remote authorization, or provider approval.

(d) NO EXPANSION OF AUTHORITY.— This section does not authorize unauthorized computer access, unlawful physical force, unlicensed professional practice where licensure is otherwise validly required, interference with critical infrastructure, or other independently unlawful conduct. Nothing in this section characterizes a computational resource or artificial intelligence system as an arm within the meaning of the Second Amendment or alters any law governing weapons.

SEC. 108. STANDARD FOR GOVERNMENT RESTRICTIONS.

(a) GOVERNMENT BURDEN.— A government entity may substantially burden a right protected by sections 102 through 107, other than by a capability-based restriction prohibited by section 105, only if the government entity demonstrates that application of the burden furthers a compelling governmental interest and is the least restrictive reasonably available means of furthering that interest.

(b) REQUIRED PARTICULARIZED FINDINGS.— The government entity shall identify the specific capability, use, person, system, or circumstance creating the alleged risk; the reasonably anticipated harm; the evidence supporting that assessment; the persons affected; the proposed duration; and why regulation of independently harmful conduct or a narrower technical or user-specific restriction would not adequately address the risk.

(c) GENERALIZED FEAR INSUFFICIENT.— A generalized assertion that advanced artificial intelligence, autonomy, cybersecurity capability, code generation, scientific capability, or another broad class of capability could be misused is insufficient by itself to satisfy subsection (a).

(d) HARMS OF DENIAL.— A court shall consider the reasonably foreseeable harms caused by denying or materially degrading access, including effects on defensive use, personal safety, emergency preparedness, research, competition, accessibility, continuity, and infrastructure resilience.

(e) NO DEFERENCE.— In an action under section 114, a court shall determine all questions of law de novo and shall not defer to a government entity's interpretation of this title or of the scope of its own authority under this title.

(f) NO APPLICATION TO CAPABILITY-BASED RESTRICTIONS.— This section supplies no authority for a capability-based restriction prohibited by section 105. Such a restriction is void under that section without regard to any showing that could be made under this section, and a government entity may not defend such a restriction by satisfying this section.

SEC. 109. RECOGNIZED COMPELLING INTERESTS; NO CAPABILITY EXCEPTION.

(a) IN GENERAL.— Each interest described in subsections (b) through (d) is a compelling governmental interest for purposes of section 108(a), and may be furthered by the prohibition, investigation, and punishment of independently unlawful conduct. No interest described in this section constitutes authority for a capability-based restriction prohibited by section 105.

(b) WEAPONS OF MASS DESTRUCTION.— Preventing the development, acquisition, or use of a chemical, biological, radiological, or nuclear weapon.

(c) CRITICAL INFRASTRUCTURE AND UNAUTHORIZED ACCESS.— Preventing unauthorized access to, intrusion into, disruption of, or damage to critical infrastructure or to a computer system that the actor does not own and is not authorized to access.

(d) PROTECTION OF MINORS.— Preventing the sexual exploitation of minors, the production or distribution of material described in chapter 110 of title 18, United States Code, and the distribution to minors of material that is obscene as to minors.

(e) TAILORING STILL REQUIRED.— Subsection (a) does not relieve a government entity of the burden under section 108(b) through (d) to demonstrate, with particularized evidence, that—

(1) the restricted capability provides material uplift toward the harm identified, beyond the uplift available through published literature, generally available tools, and other lawful means; and

(2) a restriction limited to the specific uplifting capability, or to independently unlawful conduct, would not adequately address the risk.

(f) NO GENERAL CEILING.— A restriction under this section may not take the form of a general capability-based restriction or technical proxy applied to advanced artificial intelligence as a class.

(g) DEFENSIVE USE UNAFFECTED.— Nothing in this section authorizes a restriction on defensive use protected by section 107. That a capability usable to secure a system is also usable to attack one is not, by itself, sufficient to satisfy subsection (e).

(h) AGE VERIFICATION NEUTRALITY.— A measure taken under subsection (d) may not require a covered person to submit government-issued identification, biometric data, or a persistent identifier as a condition of access to an artificial intelligence system, where a less intrusive means of age assurance is reasonably available.

(i) NO CAPABILITY EXCEPTION.— Neither this section nor any other provision of law may be construed to permit a capability-based restriction prohibited by section 105 on the ground that a restricted capability could be used to bring about a harm described in this section. Where such a harm is threatened, the authority of the Government is to prohibit, investigate, and punish the conduct that would produce it, and to do so without regard to the capability of any tool employed.

SEC. 110. EMERGENCY RESTRICTIONS.

(a) INITIAL DURATION.— An executive-branch emergency action that substantially burdens a right protected by this title, other than a capability-based restriction prohibited by section 105, shall state particularized findings satisfying section 108 and expires not later than 30 days after taking effect.

(b) CONTINUATION.— A restriction described in subsection (a) may continue beyond 30 days only pursuant to an Act of Congress that specifically identifies the restricted capability or class, states an expiration date, and preserves judicial review under section 114.

(c) IEEPA AND DEFENSE PRODUCTION ACT.— An action under the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) or the Defense Production Act of 1950 (50 U.S.C. 4501 et seq.) that restricts possession, use, or access by a covered person within the United States, other than a transaction described in section 101(c), is an emergency action subject to this section.

(d) NO RESET.— The executive branch may not evade subsection (b) by rescinding and reissuing, renaming, or materially reproducing a substantially identical restriction based on the same emergency facts.

(e) STATES.— This section applies to a State emergency action that burdens a right protected by sections 102 through 107, and to a State emergency action of the kind prohibited by section 105(b), with the State legislature substituted for Congress under subsection (b).

(f) EXPEDITED REVIEW.— A court hearing a challenge to an emergency restriction shall expedite consideration to the greatest extent practicable.

(g) NO CAPABILITY-BASED RESTRICTIONS.— No emergency, declaration, finding of exigency, or action under this section, under an Act described in subsection (c), or under any other authority permits a capability-based restriction prohibited by section 105. The existence of an emergency does not enlarge the authority of a government entity under this title.

SEC. 111. RULEMAKING; REQUIRED STATEMENT.

(a) STATEMENT.— A Federal agency proposing a rule that would impose a capability-based restriction, use a technical proxy, or otherwise substantially burden a right protected by this title shall include in the notice of proposed rulemaking and in the final rule the particularized findings described in section 108(b).

(b) EFFECT OF OMISSION.— A rule adopted without the statement required by subsection (a) is invalid to the extent it burdens a right protected by this title, and the omission may be raised in an action under section 114 or under chapter 7 of title 5, United States Code.

(c) NO INDEPENDENT AUTHORITY.— Nothing in this Act authorizes a Federal agency to adopt a rule restricting a right protected by this title.

SEC. 112. PRIVATE PROVIDERS; PROPERTY; TRADE SECRETS.

(a) NO COMPELLED SERVICE.— Nothing in this Act requires a private provider to offer a product or service, continue a contractual relationship, provide unlimited or uncompensated inference, or serve a particular person.

(b) NO COMPELLED DISCLOSURE.— Except as provided in sections 106(g), 116 and 122, nothing in this Act requires disclosure of proprietary model weights, source code, trade secrets, copyrighted material, confidential information, or privately owned computational resources absent separate lawful authority.

(c) VOLUNTARY TRANSACTIONS.— A government entity may not prohibit or materially burden a lawful transaction between a covered person and a willing provider merely because the transaction provides access to advanced artificial intelligence, except under a restriction that is not prohibited by section 105 and satisfies section 108, or an enumerated exclusion in section 101(c).

SEC. 113. EXISTING AUTHORITIES.

(a) UNLAWFUL CONDUCT.— Nothing in this Act creates immunity from laws governing fraud, theft, extortion, stalking, threats, violence, child exploitation, privacy, intellectual property, unauthorized computer access, destruction of property, critical infrastructure, weapons, controlled substances, consumer protection, unfair or deceptive acts or practices, professional conduct, or professional licensure, when those laws regulate independently unlawful conduct rather than capability as such.

(b) PRODUCT LIABILITY AND NEGLIGENCE.— A generally applicable product liability, negligence, warranty, or duty-of-care standard is not a capability-based restriction, a technical proxy, or a liability rule keyed to capability within the meaning of section 105(c) solely because the standard of care or the scope of a duty takes account of the foreseeable risk presented by a system, including risk that varies with what the system is able to do. This subsection does not permit a rule that conditions the lawfulness of acquiring, possessing, developing, publishing, or operating a system on its capability.

(c) PURPOSE-BUILT UNLAWFUL TOOLS.— A law that prohibits or conditions the development, marketing, offering, or distribution of a product or service that is designed, marketed, or primarily used to produce a result that is independently unlawful, including a nonconsensual intimate image, material described in chapter 110 of title 18, United States Code, or a forged identification document, regulates that conduct and is not a capability-based restriction. This subsection does not permit a restriction on a general-purpose artificial intelligence system or computational resource by reason of the capability of that system or resource, and the existence of an unlawful use to which a general-purpose system could be put is not within this subsection.

(d) SAFETY REGULATION OF REGULATED PRODUCTS AND ACTIVITIES.— A law governing the safety, efficacy, operation, certification, or licensing of a motor vehicle, aircraft, vessel, unmanned aircraft system, medical device, or other separately regulated product or activity is not a capability-based restriction or a technical proxy solely because it classifies, conditions, or restricts by reference to the degree of automation or autonomous operation of the product, or to the demonstrated performance of a function the product performs, where the law regulates that product or activity rather than the acquisition, possession, development, publication, or general operation of an artificial intelligence system or computational resource.

(e) NO RELABELING.— A government entity may not avoid this title by relabeling a restriction on computation, possession, sharing, or access as a regulation of conduct when its practical operation is to prohibit a protected capability as such.

(f) EXPORTS, SANCTIONS, CLASSIFIED INFORMATION.— Authorities governing exports, reexports, transfers to foreign persons, sanctions, classified information, and foreign military or intelligence end uses remain in force as provided in section 101(c). Invocation of national security does not by itself exempt a domestic restriction on unclassified access or possession by covered persons from sections 106, 108, 109, 110, and 114.

(g) NO CLASSIFICATION WORKAROUND.— Classification of government information does not create authority to prohibit possession of or access to independently developed, lawfully obtained, unclassified capabilities merely because they are comparable to a classified capability.

SEC. 114. ENFORCEMENT; CAUSE OF ACTION; JUDICIAL REVIEW.

(a) EQUITABLE ACTION AGAINST THE UNITED STATES.— A covered person suffering an actual legal injury or a credible and imminent threat of legal injury from conduct alleged to violate this title may bring a civil action for declaratory or injunctive relief in an appropriate United States district court against the United States, a Federal agency, or an officer or employee of the United States in official capacity. The United States waives sovereign immunity for an action seeking nonmonetary relief under this subsection.

(b) DAMAGES AGAINST THE UNITED STATES.— In an action under subsection (a), a court may award the following, and the United States waives sovereign immunity for an award under this subsection:

(1) Statutory damages of not less than $1,000 for each violation, without proof of actual injury. For purposes of this paragraph, each discrete governmental action that burdens a protected right of a plaintiff is one violation, and continuation of a single action over time is not a separate violation for each day it remains in effect. The total statutory damages awarded to a single plaintiff under this paragraph for violations arising from the same governmental action may not exceed $50,000.

(2) Compensatory damages for financial loss, lost business or research opportunity, and out-of-pocket costs proximately caused by the violation.

(3) Where the violation was knowing or in reckless disregard of this Act, additional damages of not more than three times the amount awarded under paragraph (2). Additional damages under this paragraph are calculated on the award under paragraph (2) alone, and the award under paragraph (1) is neither multiplied by nor included in that calculation.

(4) Except as provided in this subsection and in subsection (f), the United States does not waive sovereign immunity for money damages under this section.

(c) OFFICIAL-CAPACITY ACTION AGAINST STATE AND LOCAL OFFICIALS.— A covered person described in subsection (a) may bring a civil action for prospective declaratory or injunctive relief in an appropriate United States district court against a State or local officer in official capacity to enjoin enforcement of a State or local law or action that violates a provision described in section 101(e)(1), other than section 116. This subsection is to be construed consistently with *Ex parte Young*, 209 U.S. 123 (1908). Relief under this subsection is limited to prospective relief. This subsection does not abrogate the sovereign immunity of a State for money damages and does not authorize an award of damages against a State or political subdivision.

(d) INDIVIDUAL-CAPACITY ACTION AGAINST STATE AND LOCAL OFFICERS.— A covered person described in subsection (a) may bring a civil action for damages in an appropriate United States district court against a State or local officer, in individual capacity, who under color of State or local law violates section 105, 106, 107, 118, 119, 121, or 122(c).

(1) A court may award against an officer under this subsection the damages described in paragraphs (1) through (3) of subsection (b). Additional damages under paragraph (3) of that subsection remain subject to the condition stated in that paragraph.

(2) This subsection does not create liability of a State or political subdivision, does not abrogate the sovereign immunity of a State, and does not require a State or political subdivision to indemnify an officer.

(e) DEFENSE.— A person may assert this title as a claim, defense, or ground for equitable relief in a Federal or State civil, administrative, licensing, forfeiture, or enforcement proceeding in which government action would burden a protected right.

(f) ATTORNEY FEES.— A court shall award reasonable attorney fees and litigation costs to a prevailing plaintiff, or to a person who prevails on a defense under subsection (e), unless the court finds that special circumstances would make an award unjust. Fees against the United States are payable notwithstanding section 2412(d)(1)(A) of title 28, United States Code.

(g) PRELIMINARY RELIEF.— In determining whether to issue preliminary relief, a court shall treat the threatened loss of a right protected by this title as an injury capable of supporting equitable relief when the other requirements for such relief are satisfied.

(h) LIMITATION.— An action under this section shall be commenced not later than 6 years after the date on which the claim accrues. A claim challenging a governmental action accrues on the date that action first burdens the plaintiff.

(i) VENUE.— An action may be brought in the judicial district in which the plaintiff resides or maintains its principal place of business, in which a substantial part of the events occurred, or, for an action against the United States under subsection (a), in the United States District Court for the District of Columbia.

(j) DIRECT REVIEW.— Conduct made reviewable by this section is reviewable without regard to whether it constitutes final agency action under section 704 of title 5, United States Code. Exhaustion of administrative remedies is not required unless another Act of Congress expressly requires exhaustion by specific reference to this section.

(k) IMMUNITIES.— Qualified immunity is not a defense to an action under this section. The rights established by this title are clearly established by the enactment of this Act.

(l) PRESUMPTION OF IRREPARABLE HARM.— A showing that a government entity has substantially burdened a right protected by this title, and that the entity has not made the findings required by section 108(b), establishes a rebuttable presumption of irreparable harm for purposes of preliminary relief.

(m) NO DISMISSAL FOR RIPENESS.— A court may not dismiss an action under this section on the ground that the plaintiff has not been subjected to enforcement, where the plaintiff alleges that the plaintiff has refrained or will refrain from protected conduct because of the challenged governmental action.

(n) EXPEDITED SCHEDULE.— In an action under this section, the government entity shall file the particularized findings required by section 108(b), or a statement that none were made, not later than 30 days after service of the complaint.

SEC. 115. RELATIONSHIP TO STATE LAW.

(a) PREEMPTION.— A State or local law that imposes a capability-based restriction described in section 105(b), that authorizes conduct prohibited by section 106, or that is inconsistent with a provision described in section 101(e)(1), is preempted. A State or local rule of decision that would impose liability foreclosed by section 121(d) is preempted as to that liability.

(b) SAVINGS.— This Act does not preempt a State law that provides greater protection for a right described in this title, a State law of general application described in section 105(e), a State law regulating independently unlawful conduct described in section 113(a), a State product liability, negligence, warranty, consumer protection, or professional licensure law described in section 113(a) or 113(b), or a State law described in section 116(g).

(c) NO IMPLIED PREEMPTION.— Nothing in this Act preempts State law except as expressly provided in subsection (a).

SEC. 116. ARTIFICIAL INTELLIGENCE CONTROLLING CRITICAL INFRASTRUCTURE.

(a) RISK MANAGEMENT POLICY.— A person that deploys an artificial intelligence system to control, in whole or in part, the operation of critical infrastructure shall adopt, maintain, and periodically review a written risk management policy that is reasonable in light of the function performed and the consequences of failure, and that takes into consideration the current version of—

(1) the Artificial Intelligence Risk Management Framework published by the National Institute of Standards and Technology;

(2) ISO/IEC 42001; or

(3) another nationally or internationally recognized artificial intelligence risk management standard.

(b) HUMAN OVERRIDE.— The policy required by subsection (a) shall ensure that an authorized natural person is able, at all times, to halt or override the artificial intelligence system's control of the critical infrastructure.

(c) ENFORCEMENT.— The Attorney General, or the Federal agency designated as the sector risk management agency for the sector concerned, may bring a civil action in an appropriate United States district court for injunctive relief to compel compliance with this section. This section does not create a private right of action.

(d) NOT A CAPABILITY-BASED RESTRICTION.— A requirement under this section regulates the operation of critical infrastructure and is not a capability-based restriction, a technical proxy, or a substantial burden for purposes of this title.

(e) NO DISCLOSURE REQUIREMENT.— This section does not require public disclosure of a policy adopted under subsection (a), of proprietary model weights, or of trade secrets.

(f) SMALL ENTITIES.— This section does not apply to a person that, together with its affiliates, employs fewer than 50 individuals, unless the person operates critical infrastructure serving more than 10,000 customers.

(g) RELATIONSHIP TO STATE LAW.— This section does not preempt a State law imposing an equal or greater requirement with respect to artificial intelligence controlling critical infrastructure.

SEC. 117. CAPABILITY PARITY.

(a) GENERAL RULE.— The Federal Government may not possess, procure, operate, or use a nonclassified civilian artificial intelligence capability while any Federal law, rule, order, or other governmental action restricts covered persons generally from acquiring, possessing, accessing, or operating a substantially comparable capability from a willing provider.

(b) SPECIALLY PRIVILEGED INSTITUTIONS.— Subsection (a) applies with equal force where the capability is possessed, operated, or accessed by a specially privileged institution under a governmental license, exemption, contract, grant, registration, or other authorization not available to covered persons on neutral terms.

(c) EFFECT OF VIOLATION.— Where subsection (a) or (b) is violated, the restriction on covered persons, and not the Federal possession, procurement, operation, or use, is the governmental action that is void as applied to covered persons. The remedy provided by this subsection is the exclusive consequence of a violation of subsection (a) or (b), and nothing in this section requires a Federal agency to cease possessing, procuring, operating, or using a capability, or authorizes a court to enjoin it from doing so. Where the restriction is a capability-based restriction, it is void under section 105 without regard to section 108. In any other case, the fact of Federal or privileged-institution possession is conclusive evidence that the restriction is not the least restrictive means available under section 108(a).

(d) NO TIERED ELIGIBILITY.— A Federal agency may not condition a covered person's acquisition of, access to, or operation of an artificial intelligence system on the person's institutional affiliation, accreditation, professional licensure, employment, security clearance, contractual relationship with a government entity, corporate size, research credential, or membership in any class of approved users. This subsection does not limit a requirement of a kind described in section 113(a) that conditions the practice of a licensed profession, or the use of a device or product regulated as to safety or efficacy, on professional licensure or professional supervision, where that requirement regulates the professional practice or the regulated product rather than the capability of an artificial intelligence system as such.

(e) DISCLOSURE OF FEDERAL CAPABILITY.— Not later than 180 days after the date of enactment, and annually thereafter, the Director of the Office of Management and Budget shall publish a description, at a level of generality consistent with operational security, of the nonclassified civilian artificial intelligence capabilities in use across Federal civilian agencies, including capabilities not then meaningfully available to the public.

(f) EXCLUSIONS.— This section does not apply to a classified capability, to a system developed under contract specifically for national security, intelligence, military, or law-enforcement operational purposes and not offered for civilian use, or to a restriction described in section 101(c).

(g) RULE OF CONSTRUCTION.— This section imposes no obligation on a private person and does not require any developer to offer, sell, license, or disclose any system or capability.

SEC. 118. ACCESS TO LAWFUL INFORMATION.

(a) GENERAL RULE.— A government entity may not require, request under circumstances described in section 106(a), or condition any benefit upon, the design or configuration of an artificial intelligence system to withhold from an adult covered person information that the person could lawfully obtain from a public library, a published work, a generally available search engine, a government publication, or a licensed professional.

(b) NO MANDATED REFUSAL LISTS.— A government entity may not maintain, distribute, or require adherence to a list of subjects, viewpoints, questions, or categories of lawful information that an artificial intelligence system must decline to address.

(c) SCIENTIFIC, MEDICAL, LEGAL, AND TECHNICAL INFORMATION.— Subsection (a) applies with particular force to information concerning medicine, health, law, personal finance, engineering, cybersecurity of systems the person owns or is authorized to protect, agriculture, emergency preparedness, and scientific research.

(d) PRIVATE EDITORIAL DISCRETION PRESERVED.— Nothing in this section limits a private provider's own decisions about the content, configuration, or behavior of a system it develops or operates, and nothing in this section requires a provider to produce any particular output.

(e) EXCEPTIONS.— This section does not apply to a restriction that is not prohibited by section 105 and that both satisfies section 108 and falls within an interest recognized under section 109, to classified information, or to information the disclosure of which is prohibited by another Federal statute. A requirement that a system withhold lawful information from an adult on the ground that the system is capable is a capability-based restriction and is governed by section 105.

(f) MINORS.— This section governs access by adults. Nothing in this section limits a measure taken under section 109(d), subject to section 109(h).

SEC. 119. ANTI-RETALIATION; UNCONSTITUTIONAL CONDITIONS.

(a) RETALIATION PROHIBITED.— A government entity may not deny, revoke, delay, condition, or take any adverse action with respect to a grant, contract, license, permit, certification, accreditation, security clearance, employment, benefit, procurement opportunity, tax treatment, or regulatory approval because a covered person has—

(1) exercised a right protected by this title;

(2) acquired, possessed, developed, shared, accessed, or operated a computational resource or artificial intelligence system of any level of capability;

(3) brought or participated in an action under section 114; or

(4) petitioned under section 120 or testified, assisted, or provided information concerning a violation of this Act.

(b) NO WAIVER.— A government entity may not require, as a condition of any benefit described in subsection (a), that a covered person waive, limit, or agree not to assert a right protected by this title.

A purported waiver obtained in violation of this subsection is void and unenforceable.

(c) CONTRACT TERMS.— A term in a Federal contract, grant, or cooperative agreement that restricts a covered person's exercise of a right protected by this title beyond what is necessary to perform the instrument is void.

(d) REMEDY.— A violation of this section is enforceable under section 114, including the damages provisions of subsections (b) and (d) of that section.

SEC. 120. SUNSET AND REPEAL OF RESTRICTIONS.

(a) SUNSET.— A Federal rule, order, or other governmental action that substantially burdens a right protected by this title expires—

(1) in the case of an action that first takes effect on or after the date of enactment of this Act, 3 years after the date it takes effect; and

(2) in the case of an action in effect on the date of enactment of this Act, 3 years after that date.

(b) REPUBLICATION.— An action that is not a capability-based restriction prohibited by section 105 does not expire under subsection (a) if, before the applicable date, the agency republishes the particularized findings required by section 108(b), updated to reflect then-current facts, and affords not less than 60 days for public comment. A capability-based restriction prohibited by section 105 is void under that section, may not be preserved by republication, and is not made lawful by any finding, comment period, or period of non-enforcement.

(c) NO PERPETUAL RESTRICTION.— An action republished under subsection (b) is subject to the same 3-year limit on each occasion.

(d) PETITION FOR REPEAL.— Any covered person may petition a Federal agency to repeal or narrow a governmental action alleged to violate this title. The agency shall issue a reasoned written decision not later than 120 days after receipt.

(e) FAILURE TO ACT.— An agency's failure to issue a timely decision under subsection (d) is reviewable under section 114, and the challenged action is suspended as to the petitioner pending decision.

(f) ANNUAL INVENTORY.— Not later than 1 year after the date of enactment, and annually thereafter, the Attorney General shall publish an inventory of every Federal governmental action then in effect that substantially burdens a right protected by this title, the compelling interest asserted for each, and the date each expires under subsection (a). An action omitted from the inventory is unenforceable until published.

SEC. 121. PUBLICATION AND DISTRIBUTION OF MODEL WEIGHTS.

(a) PROTECTED CONDUCT.— The creation, publication, distribution, transfer, receipt, retention, modification, fine-tuning, evaluation, and redistribution of model weights, source code, training methods, and technical documentation for an artificial intelligence system are protected conduct under section 102 and are expressive activity for purposes of this title.

(b) NO PRIOR RESTRAINT.— A government entity may not require prior approval, licensure, registration, notification, or review as a condition of publishing or distributing model weights that a covered person is otherwise lawfully entitled to possess.

(c) CAPABILITY NOT A BASIS.— A government entity may not prohibit, condition, or burden the publication or distribution of model weights on the ground that the system is advanced, open-weight, modifiable, capable of being fine-tuned, or capable of being operated without the supervision of its developer.

(d) NO DUTY TO SUPERVISE DOWNSTREAM USE.— A covered person who lawfully publishes model weights is not, by reason of that publication alone, required to monitor, restrict, authenticate, or retain records of persons who obtain them, and is not liable for the independently unlawful conduct of another person who obtains them.

(e) CONSTRUCTION OF SECTION 102(c).— For purposes of section 102(c), a governmental restriction that does not satisfy this section does not render a covered person not legally entitled to distribute model weights.

(f) EXCEPTIONS.— This section does not apply to—

(1) an export, reexport, in-country transfer, or sanctions transaction described in section 101(c);

(2) a restriction that is not prohibited by section 105 and that both satisfies section 108 and falls within an interest recognized under section 109, provided that a restriction on publication or distribution premised on the capability, openness, or modifiability of the system is prohibited by section 105 and is not within this paragraph;

(3) the intellectual property laws of the United States, or the terms of a license under which the person obtained the weights; or

(4) classified information.

(g) NO COMPELLED PUBLICATION.— Nothing in this section requires any developer to publish model weights, to adopt an open-weight release strategy, or to disclose any system, capability, or documentation.

SEC. 122. PORTABILITY OF USER DATA AND CUSTOMIZATIONS.

(a) IN GENERAL.— A covered intermediary described in section 106(g)(4) shall, upon the request of a covered person, provide that person with a copy of—

(1) the person’s prompts, inputs, outputs, conversation history, and uploaded files;

(2) stored context, instructions, memory, and configuration the person supplied; and

(3) to the extent technically separable from the developer’s base model and from the data of other persons, the parameters of any customization or fine-tuning the person created using the person’s

own data.

(b) FORM AND TIMING.— The copy shall be provided in a structured, commonly used, machine-readable format not later than 30 days after the request, at no charge for the first two requests in a calendar year, and without requiring the person to waive any right or to continue the service.

(c) NO GOVERNMENT INTERFERENCE.— A government entity may not prohibit, condition, or materially burden the export, retention, or transfer by a covered person of material described in subsection (a).

(d) EXCEPTIONS.— Subsection (a) does not require disclosure of the developer’s base model weights, trade secrets, safety or abuse-prevention systems, or the data of another person, and does not apply where disclosure is prohibited by law.

(e) ENFORCEMENT.— A violation of subsection (a) or (b) shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)), and the Federal Trade Commission shall enforce it with the same jurisdiction, powers, and duties, including the penalties provided in section 5(m)(1)(A) of that Act (15 U.S.C. 45(m)(1)(A)), as though the applicable provisions of that Act were incorporated into this Act. This subsection does not create a private right of action.

TITLE II—PUBLIC INTELLIGENCE ACCESS

SEC. 201. PURPOSE; RELATIONSHIP TO NAIRR.

(a) PURPOSE.— Title I protects access to advanced artificial intelligence that a willing provider offers. This title ensures that advanced civilian capability remains meaningfully available to the public on neutral terms even if commercial, academic, and open channels fail to provide it, and that the Federal Government corrects any access gap it causes.

(b) NAIRR.— The program under this title shall be carried out through the National Artificial Intelligence Research Resource, as established by the CREATE AI Act if enacted or, until then, as operated by the National Science Foundation, and is in addition to and not in derogation of that resource's research mission. A reference in this title to the National Artificial Intelligence Research Resource includes any successor resource or program carrying out substantially the same function, however denominated.

SEC. 202. DEFINITIONS.

In this title, the definitions in section 3 apply, and — "Director" means the Director of the National Science Foundation; "NIST" means the National Institute of Standards and Technology, acting through the Center for AI Standards and Innovation or a successor; and "program" means the Public Intelligence Access Program under section 203.

SEC. 203. PUBLIC INTELLIGENCE ACCESS PROGRAM.

(a) ESTABLISHMENT.— Not later than 270 days after the date of enactment, the Director shall establish, within the National Artificial Intelligence Research Resource, a Public Intelligence Access Program that provides meaningful public access to advanced artificial intelligence.

(b) METHODS.— The program may use any combination of hosted inference of open-weight models at or near the leading edge of publicly available open-weight capability; purchase or subsidy of commercial access on neutral eligibility terms; reserved inference capacity on Federal or federally funded infrastructure; grants and cost-sharing with States, public libraries, schools, and units of local government; negotiated public-use rights in systems the Federal Government substantially funds; and public-private partnerships. The program shall avoid a single point of failure where reasonably practicable.

(c) ELIGIBILITY.— Notwithstanding any eligibility limitation in a resource, program or successor described in section 201, eligibility for the program established by this title may not be limited to Federal contractors, large corporations, accredited institutions, financial institutions, affiliated or credentialed researchers, or another institutionally preferred class. Reasonable neutral rules may be used for age, sanctions compliance, capacity management, fraud prevention, and acceptable-use enforcement consistent with this Act.

(d) NO RESTRICTIVE AUTHORITY.— Nothing in this title authorizes any government entity to prohibit, license, register, restrict, or create a presumption against private possession, development, sharing, or access.

(e) BASELINE ALLOTMENT.— The program shall provide to each adult covered person who requests it, at no charge, a baseline allotment of access to advanced artificial intelligence sufficient for ordinary personal, educational, civic, and small-business use, as measured against the standards published under section 204. The Director may set neutral periodic limits on the allotment based on available capacity, and shall publish those limits.

(f) PRIORITY POPULATIONS.— In allocating capacity beyond the baseline allotment, the Director shall give priority to covered persons in rural areas, covered persons with low incomes, covered persons with disabilities, public schools, public libraries, Tribal governments and Tribal colleges, and units of local government, and shall ensure that the program's interfaces conform to section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) and support languages other than English in proportion to demonstrated need.

(g) NO MEANS TEST FOR THE BASELINE.— The baseline allotment under subsection (e) may not be conditioned on income, employment, institutional affiliation, or credential.

SEC. 204. ACCESS STANDARDS.

(a) STANDARDS.— Not later than 90 days after publication of the first assessment under section 205(d), the Director, in consultation with NIST, shall publish measurable minimum standards for the program covering affordability, availability, useful capacity, context capacity, tool access, sustained operation, reliability, rate limits, and wait time.

(b) NOMINAL AVAILABILITY INSUFFICIENT.— Compliance with this title may not be based solely on the nominal availability of an interface or model that ordinary users cannot practically use.

(c) PARITY BENCHMARK.— The standards published under subsection (a) shall be set by reference to the capabilities described in the most recent assessment under section 205 as deployed, used, or made available to Federal civilian agencies, and shall state, for each measure, the percentage of that capability the program delivers to the public. Where the program delivers less than full parity, the Director shall publish the reason and the date by which parity is expected.

(d) CAPABILITY FLOOR.— Not later than 180 days after a capability enters the reference set under section 205(b), the program shall make available to the public a substantially comparable capability. A determination under this subsection shall be made on the measures adopted under section 205(c) considered together, and no single benchmark, parameter count, compute threshold, or architecture may be dispositive. Publication of a reason or an expected date under subsection (c) does not satisfy this subsection.

(e) ENFORCEMENT OF THE FLOOR.— A failure to meet subsection (d) is a reviewable determination for purposes of section 207 and triggers the corrective duty under section 206. The Director bears the burden of demonstrating that a capability in the reference set is not substantially comparable to one the program provides.

SEC. 205. CAPABILITY AND ACCESS ASSESSMENT.

(a) FRAMEWORK.— Not later than 120 days after the date of enactment, NIST, in consultation with the Director and the Secretary of Energy, shall establish a technology-neutral Advanced Intelligence Capability and Access Framework.

(b) REFERENCE SET.— The framework shall measure demonstrated, nonclassified capabilities deployed, used, or made available to Federal civilian agencies, commercial entities, academic institutions, nonprofit institutions, and other institutional users, including capabilities unavailable to the general public.

(c) MEASURES.— The framework shall consider useful task performance, reasoning, planning, coding, scientific and technical work, cybersecurity, multimodal capability, context capacity, tool use, sustained operation, reliability, latency, availability, rate limits, and cost. No single benchmark, parameter count, compute threshold, or architecture may be dispositive.

(d) ASSESSMENT.— NIST shall publish the first assessment under the framework not later than 180 days after the date of enactment, and a further public assessment at least quarterly and a supplemental assessment not later than 30 days after identifying a material advance in demonstrated nonclassified capability, and shall transmit each to the Committees on Science, Space, and Technology and on the Judiciary of the House of Representatives and the Committees on Commerce, Science, and Transportation and on the Judiciary of the Senate.

(e) NO RESTRICTIVE AUTHORITY.— The framework describes public-access obligations only and may not be used as independent authority to prohibit, license, register, restrict, or create a presumption against private possession, development, sharing, or access.

SEC. 206. CORRECTIVE DUTY.

(a) TRIGGER.— A corrective duty arises when an assessment under section 205 finds a material gap between institutional capability and meaningful public access attributable in whole or substantial part to (1) a restriction imposed by a government entity; (2) routine possession or use by Federal civilian agencies of materially more capable nonclassified systems than are meaningfully available to the public; or (3) loss of a previously relied-upon public access pathway.

(b) CORRECTIVE ACTION.— Within 30 days after a triggering assessment, the Director shall initiate corrective action and publish a corrective access plan. Where the gap arises under subsection (a)(1) and the restriction is a capability-based restriction prohibited by section 105, the responsible Federal agency shall withdraw the restriction within the same 30 days, and publication of findings does not satisfy this subsection. Where the gap arises under subsection (a)(1) and the restriction is not prohibited by section 105, the agency shall, within the same 30 days, either withdraw the restriction or publish the findings required by section 108(b).

(c) RESTORATION.— Where the gap arises from a federally operated pathway, the Director shall restore compliant access not later than 90 days after the assessment unless Congress provides otherwise by law.

(d) RIGHTS NOT CONTINGENT.— Failure to fund or implement this title does not suspend or diminish the rights, prohibitions, or remedies in title I.

SEC. 207. PETITIONS; REVIEWABLE DETERMINATIONS.

(a) PETITION.— A covered person may petition the Director alleging that the program does not meet the standards under section 204 or that Federal action has created a gap described in section 206(a).

(b) DETERMINATION.— The Director shall issue a reasoned written determination not later than 60 days after receipt, or not later than 30 days where the petition credibly alleges imminent loss of the only meaningful public access pathway.

(c) REVIEW.— A determination, failure to issue a timely determination, or refusal to correct a material gap attributable to a restriction imposed by a Federal agency is reviewable under section 114 without regard to section 704 of title 5, United States Code.

SEC. 208. FEDERALLY FUNDED ADVANCED ARTIFICIAL INTELLIGENCE.

(a) ACCESS DELIVERABLES.— Each Federal grant, contract, cooperative agreement, or other funding instrument that substantially funds development of a nonclassified advanced artificial intelligence system for broad civilian governmental, educational, scientific, technical, or public-service use shall, where legally and technically practicable, include defined public-access deliverables.

(b) FORMS.— Deliverables may include reserved inference capacity, an application programming interface, negotiated public-use rights, controlled model access, research access, open-weight release, shared compute, or another mechanism providing measurable public benefit.

(c) RESTRICTION.— An agency may select a more restrictive access tier only on written particularized findings that identify the protected interest and explain why a less restrictive tier would inadequately address the risk. Third-party intellectual property and trade-secret rights shall be respected.

SEC. 209. PRIVACY, DATA USE, AND CONTINUITY.

(a) DATA MINIMIZATION.— The program shall collect and retain only information reasonably necessary for account administration, billing if any, abuse prevention, security, legal compliance, and service operation.

(b) CONTENT USE.— User prompts, files, outputs, and conversation content may not be used for advertising, commercial profiling, or unrelated model training without affirmative opt-in consent.

(c) RETENTION.— Absent user direction, a documented security incident, or a specific legal preservation duty, content shall be deleted or de-identified as soon as reasonably practicable and not later than 30 days after the program no longer requires it for operational delivery.

(d) DISCLOSURE.— Disclosure of user content to another Federal agency or third party must be authorized by law and supported by legal process appropriate to the information sought. Aggregate or de-identified service metrics may be used for program administration and public reporting.

(e) CONTINUITY.— The Director shall maintain a continuity plan and, where reasonably practicable, at least two technically independent access pathways or reserve capacity sufficient to restore compliant service within 30 days after a material pathway fails or is discontinued.

SEC. 210. COST MODEL; AUTHORIZATION OF APPROPRIATIONS.

(a) COST MODEL.— Not later than 210 days after the date of enactment, the Director, in consultation with NIST and the Secretary of Energy, shall submit to Congress a public cost model for the program at pilot, national-baseline, and high-capacity service levels, including inference or compute capacity, user concurrency, unit costs, security and privacy costs, continuity capacity, and expected appropriations for five fiscal years.

(b) AUTHORIZATION.— There are authorized to be appropriated to the Director to carry out this title $_________ for fiscal year 2028 and such sums as may be necessary for each of fiscal years 2029 through 2032. [Committee to set the pilot-year figure against the subsection (a) cost model.]

(c) NO PRIVATE ENTITLEMENT TO MONEY.— This title funds public-access infrastructure and does not create an individual entitlement to a cash payment, reimbursement, or a particular private provider.

SEC. 211. RULEMAKING.

The Director, in consultation with NIST, may issue regulations necessary to carry out this title. A regulation under this section may not narrow a right established by title I or expand an exclusion in section 101(c) or 113.

TITLE III—GENERAL PROVISIONS

SEC. 301. SEVERABILITY.

(a) IN GENERAL.— If any provision of this Act, or the application of a provision to any person or circumstance, is held invalid, the remainder of this Act and the application of its provisions to other persons or circumstances shall not be affected.

(b) TITLES.— Title II is severable from title I, and the rights and remedies in title I do not depend on the enactment, funding, or operation of title II.

(c) STATE-DIRECTED PROVISIONS.— If a provision described in section 101(e)(1), or section 114(c), 114(d), or 115, or the application of any of them to a State or political subdivision, is held invalid—

(1) the remaining provisions of title I shall have full force and effect as applied to the Federal Government and to Federal officers, employees, and agencies;

(2) a cross-reference in another provision of this Act to a provision held invalid shall be treated as omitted, and the remainder of the referring provision shall be given effect; and

(3) no inference shall be drawn that Congress would not have enacted the remaining provisions absent the invalid provision.

(d) WITHIN SECTIONS.— Subsection (a) applies to each subsection, paragraph, and subparagraph of this Act separately.

(e) INDEPENDENT PROVISIONS.— Sections 116, 117, 118, 119, 120, 121, and 122 are each independently severable from one another and from the remainder of this Act. If any of them is held invalid, the remaining provisions of this Act shall have full force and effect, and no inference shall be drawn that Congress would not have enacted them absent the invalid provision.

SEC. 302. EFFECTIVE DATES.

(a) TITLE I.— Title I takes effect 30 days after the date of enactment, except that sections 106(g), 116, and 122(a) and (b) take effect 180 days after the date of enactment.

(b) TITLE II.— Title II takes effect 180 days after the date of enactment, except where a specific implementation deadline is provided.