

(1) apply to civil defamation, slander, or libel claims or defenses under State law, regardless of whether or not such claims or defenses, respectively, are raised in a State or Federal court; or

(2) prevent the Federal Government from pursuing an investigation of a covered journalist or organization that is—

(A) suspected of committing a crime;

(B) a witness to a crime unrelated to engaging in journalism;

(C) suspected of being an agent of a foreign power, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 ([50 U.S.C. 1801](#));

(D) an individual or organization designated under Executive Order 13224 ([50 U.S.C. 1701 note](#); relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism);

(E) a specially designated terrorist, as that term is defined in section 595.311 of title 31, Code of Federal Regulations (or any successor thereto); or

(F) a terrorist organization, as that term is defined in section 212(a)(3)(B)(vi)(II) of the Immigration and Nationality Act ([8 U.S.C. 1182\(a\)\(3\)\(B\)\(vi\)\(II\)](#)).

Subtitle C—Government and Artificial Intelligence

SEC. 1031. FINDINGS AND PURPOSE.

(a) Findings.—Congress finds the following:

(1) Artificial intelligence presents a significant opportunity to improve public administration, expand access to services, strengthen security, support scientific and technical progress, and promote the general welfare of the people of the United States.

(2) Because artificial intelligence can influence decisions affecting rights, liberties, safety, privacy, property, the use of force, and access to essential opportunities and services, the Government bears a special responsibility to ensure that its use of artificial intelligence remains lawful, intelligible, accountable, and subject to meaningful human judgment.

(3) The Federal Government can minimize public dependence on a small number of dominant tech companies and promote competition policy by setting procurement standards that promote interoperability, portability, auditability, and technical independence over opaque and locked systems.

(b) Purpose.—The purpose of this subtitle is to establish public policy for the United States governing artificial intelligence that reflects the highest ideals of the United States, including—

(1) enabling the beneficial use of artificial intelligence to improve public administration, reduce administrative burden, strengthen security, expand access to services, support scientific and technical progress, and help public servants serve the people of the United States more effectively; and

(2) establishing safeguards against uses of artificial intelligence that are inconsistent with constitutional government, including mass surveillance, social scoring, unlawful delegation of lethal force, covert manipulation of the public, and other uses that threaten rights, liberties, privacy, safety, or democratic self-government.

SEC. 1032. FEDERAL ARTIFICIAL INTELLIGENCE AND TECHNOLOGY TALENT TEAMS.

(a) Definitions.—In this section:

(1) Agency.—The term "agency" means an agency described in [section 901\(b\) of title 31](#), United States Code.

(2) Examination.—The term "examination"—

(A) means an opportunity to directly demonstrate knowledge, skills, abilities, and competencies for a position through an assessment;

(B) includes a resume review that is—

(i) conducted or informed by a subject matter expert; and

(ii) based upon indicators that—

(I) are derived from a job analysis; and

(II) bear a rational relationship to performance in the position for which the examining agency is making an appointment; and

(C) on and after July 1, 2031, does not solely include or principally rely upon a self-assessment from an automated examination, except as provided in subsection (e).

(3) Examining agency.—The term "examining agency" means—

(A) the Office of Personnel Management; or

(B) an agency to which the Director of the Office of Personnel Management has delegated examining authority under [section 1104\(a\)\(2\) of title 5](#), United States Code.

(4) Subject matter expert.—The term "subject matter expert" means an employee or selecting official—

(A) who possesses understanding of the duties of, and knowledge, skills, and abilities required for, the position for which the employee or selecting official is developing or administering an assessment; and

(B) whom the agency that employs the employee or selecting official designates to assist in the development and administration of technical assessments under subsection (d).

(5) Technical assessment.—The term "technical assessment" means an assessment developed under subsection (d) that—

(A) allows for the demonstration of job-related technical skills, abilities, and knowledge;

(B) is based upon a job analysis and is relevant to the position for which the assessment is developed; and

(C) may include—

(i) a structured interview;

(ii) a work-related exercise;

(iii) a custom or generic procedure used to measure an individual's employment or career-related qualifications and interests;

(iv) another assessment that meets the criteria under subparagraphs (A) and (B);

(v) external industry assessments, including multi-hurdle or skills-based assessments; or

(vi) coding tests, automated transcription, or flexible timed exercises.

(b) Federal agency technology and artificial intelligence talent teams.—

(1) In general.—An agency may establish 1 or more technology and artificial intelligence talent teams, including at the component level.

(2) Composition.—A technology and artificial intelligence talent team under this subsection may consist of shared certificate coordinators, recruiters, assessment experts, subject matter experts, and nontechnical positions that enable artificial intelligence governance, innovation, and risk management.

(3) Duties.—A technology and artificial intelligence talent team under this subsection shall provide hiring support to the agency and other agencies for technology and artificial intelligence positions, including by—

(A) improving examinations for such positions;

(B) facilitating writing job announcements for such positions in the competitive service;

(C) sharing high-quality certificates of eligibles; and

(D) facilitating hiring for such positions in the competitive service using examinations and subject matter experts.

(4) Other teams.—An agency may establish centralized guidance and practices to support agency-led talent teams in order to address high-need hiring areas.

(c) Office of Personnel Management team.—

(1) In general.—The Director of the Office of Personnel Management may establish a Federal technology and artificial intelligence talent team to support agency talent teams in facilitating pooled hiring actions for technology and artificial intelligence talent across the

Federal Government, providing training, and creating technology platforms to facilitate hiring for the competitive service, including by—

(A) ensuring agencies are using best practices for technology and artificial intelligence hiring;

(B) leading cross-Government hiring efforts for technology and artificial intelligence hiring and engagement with key candidates;

(C) developing technical assessments; and

(D) sharing certificates of eligibles and accompanying résumés under sections [3318\(b\)](#) and [3319\(c\)](#) of title 5, United States Code.

(2) Other teams.—The Director of the Office of Personnel Management—

(A) may establish other talent teams to address high-need hiring areas at any agency; and

(B) may expand the hiring experience team at the Office of Personnel Management to focus on surge hiring and scaling pooled hiring, with initial focus on artificial intelligence and artificial intelligence-enabling roles.

(d) Technical assessments.—

(1) In general.—For the purpose of conducting an examination for technology and artificial intelligence positions in the competitive service, a subject matter expert may—

(A) develop, in partnership with human resources employees of the examining agency, a position-specific assessment that is relevant to the position; and

(B) administer the assessment developed under subparagraph (A) to—

(i) determine whether an applicant for the position has demonstrated the established qualifications for the position; or

(ii) rank applicants for the position for category rating purposes under [section 3319 of title 5](#), United States Code.

(2) Sharing and customization of assessments.—

(A) Sharing.—An examining agency may share a technical assessment under this subsection with another examining agency if each agency maintains appropriate control over examination material.

(B) Customization.—An examining agency with which a technical assessment is shared under subparagraph (A) may customize the assessment as appropriate, provided that the resulting assessment satisfies the requirements under part 300 of title 5, Code of Federal Regulations, or any successor regulation.

(C) Platform for sharing and customization.—

(i) In general.—The Director of the Office of Personnel Management shall establish and operate an online platform on which examining agencies may share and customize technical assessments under this subsection.

(ii) Platform requirements.—The Director of the Office of Personnel Management—

(I) shall not be responsible for independently validating the utility of the content and technical assessments shared on the platform described in clause (i); and

(II) shall ensure that the platform includes the ability of its users to rate the utility of the content and technical assessments shared on the platform to allow for a ranking of such content and assessments.

(3) Existing platforms.—If practicable, an agency shall use an existing hiring platform, including the USA Hire platform, to conduct technical assessments.

(e) Waiver of restriction on automated examinations.—

(1) Chief Human Capital Officer.—The Chief Human Capital Officer of an agency may waive subsection (a)(2)(C) if, not later than 30 days after the date on which the Officer authorizes the waiver, the Officer submits to the Director of the Office of Personnel Management a written report that justifies the need for the waiver and articulates the data, evidence, and circumstances for that need.

(2) Office of Personnel Management.—The Director of the Office of Personnel Management—

(A) may provide agencies with guidance and instruction on the data, evidence, and circumstances that should be included in a waiver under paragraph (1); and

(B) not later than 30 days after the date on which the Director receives a waiver under paragraph (1), shall post the waiver on a public website.

(3) Effect.—A waiver authorized under paragraph (1) shall not take effect until the Director of the Office of Personnel Management posts the waiver under paragraph (2)(B).

SEC. 1033. PROHIBITED GOVERNMENT USES OF ARTIFICIAL INTELLIGENCE.

(a) Definitions.—In this section:

(1) Aggrieved person.—The term "aggrieved person" means any person who is the target of, or materially affected by, surveillance or other conduct in violation of this section.

(2) Artificial intelligence.—The term "artificial intelligence" has the meaning given that term in section 581.

(3) Artificial intelligence-enabled surveillance system.—The term "artificial intelligence-enabled surveillance system" means any artificial intelligence system, algorithmic system, or computational process used to identify, track, monitor, infer, classify, predict, score, map, or analyze persons, groups, communications, movements, associations, activities, or patterns of life using personal data, biometric data, communications data, geolocation data, transactional data, publicly available information, or other data.

(4) Behavioral inference.—The term "behavioral inference" means any inference, prediction, or assessment concerning a person's intentions, beliefs, associations, emotions, mental state, likely future conduct, or other behavioral characteristics derived from data analysis, pattern recognition, or artificial intelligence.

(5) Biometric identification.—The term "biometric identification" means identification or attempted identification of a person based on face, voice, gait, iris, retina, fingerprint, palm print, hand geometry, vein pattern, DNA, or any other biological, physiological, or behavioral characteristic used to identify or verify identity.

(6) Federal agency.—The term "Federal agency" means any Executive agency, as defined in [section 105 of title 5](#), United States Code, and includes any military department.

(7) Meaningful human control.—The term "meaningful human control" means a level of human involvement in a decision to use lethal force that ensures that—

(A) a human commander or operator has sufficient information about the target, the system, and the operational context to make an informed judgment as to the lawfulness, necessity, and proportionality of each individual use of lethal force;

(B) the commander or operator has a genuine opportunity to approve or withhold approval of each individual use of lethal force before lethal force is applied; and

(C) the commander or operator retains the ability to supervise the system, to intervene, and to deactivate or abort the use of lethal force in real time where technologically feasible.

(8) Persistent tracking.—The term "persistent tracking" means tracking a person's location, movement, associations, activities, or interactions over time, whether continuously or intermittently, in a manner sufficient to reveal a pattern of life.

(9) Population-scale monitoring.—The term "population-scale monitoring" means monitoring, screening, scanning, scoring, or analyzing multiple persons or groups on a dragnet, bulk, mass, or generalized basis, rather than on the basis of individualized suspicion concerning a specifically identified person.

(10) Publicly accessible space.—The term "publicly accessible space" means any place, facility, forum, platform, website, service, or area, whether physical or digital, that is generally open to, or ordinarily used by, the public.

(11) Social scoring system.—The term "social scoring system" means any artificial intelligence-enabled or algorithmic system that ranks, classifies, rewards, penalizes, predicts, or otherwise evaluates the trustworthiness, risk, compliance, loyalty, character, or social value of a person based on aggregated behavior, associations, speech, movement, communications, purchasing patterns, travel activity, mailing patterns, financial activity, or other personal data.

(b) Prohibited uses.—Except as expressly authorized under subsection (f), no Federal agency may acquire, possess, deploy, access, use, or materially rely on an artificial intelligence-enabled surveillance system for any of the following purposes:

(1) Real-time or near-real-time biometric identification, or biometric identification based on recorded footage, in any publicly accessible space.

(2) Persistent identification, persistent tracking, behavioral inference, pattern-of-life analysis, or population-scale monitoring of persons in the United States.

(3) Persistent or automated cross-system linking of license plate data, facial images, gait, voice, device identifiers, geolocation data, communications metadata, mailing patterns, financial transactions, travel records, or other identifying or pseudonymous data for the purpose of tracking, monitoring, mapping, or scoring persons over time.

(4) Dragnet monitoring, scraping, or analysis of social media, communications, mailing patterns, financial activity, travel activity, purchasing activity, or other associative data to identify, map, predict, or score lawful speech, protest, assembly, association, religious exercise, political activity, journalistic activity, or other constitutionally protected activity.

(5) Suppressing, penalizing, chilling, deterring, or otherwise burdening lawful speech, protest, assembly, association, petition, or other constitutionally protected activity.

(6) Inferring, predicting, or assigning a person's beliefs, intentions, ideology, associations, emotions, mental state, immigration status, health status, disability status, or other protected or highly sensitive characteristics for purposes of law enforcement, immigration enforcement, benefits administration, employment decisions, licensing, or any other adverse government action.

(7) Inferential assignment by artificial intelligence as a substitute for lawful adjudication with respect to immigration status, disability status, health status, fraud status, threat status, or other legal or factual predicates for adverse government action.

(8) Predictive policing, threat scoring, risk scoring, or similar predictive or classificatory systems not based on individualized suspicion and judicial authorization.

(9) Using artificial intelligence-generated or artificial intelligence-amplified accounts, avatars, personas, or other automated systems to impersonate private persons or to covertly influence public discourse, public opinion, or civic participation on behalf of the Federal Government.

(c) Prohibition on social scoring.—

(1) In general.—No Federal agency may create, maintain, purchase, use, or materially rely on any social scoring system.

(2) Rule of construction.—A system shall not be excluded from paragraph (1) merely because it is described as an eligibility score, trust and safety score, threat score, credibility score, behavior score, fraud score, or by any similar label.

(d) Prohibition on lethal force.—No Federal agency may use artificial intelligence, or any sensor, biometric, behavioral, machine-learning, pattern-recognition, or other computational output, to select a human being for lethal engagement, prioritize a human being for lethal engagement, recommend lethal engagement of a human being, or engage a human being with lethal force, unless each individual use of lethal force remains subject to meaningful human control.

(e) Funding, anti-circumvention, procurement, and public communications.—

(1) Funding prohibition.—No Federal funds appropriated or otherwise made available may be obligated or expended to acquire, possess, deploy, access, use, materially rely on, or otherwise support any activity prohibited under subsections (b) through (d), or to obtain data, services, outputs, inferences, analyses, leads, alerts, or other products derived from such activity.

(2) Anti-circumvention.—A Federal agency may not do indirectly, through a State, political subdivision, contractor, subcontractor, grantee, cooperative agreement, memorandum of understanding, information sharing arrangement, data broker, or other third party, what such agency may not do directly under subsections (b) through (d).

(3) Auditability requirement.—No Federal agency may procure, license, subscribe to, access, use, or materially rely on any artificial intelligence-enabled surveillance system if the terms of use, technical design, or contractual restrictions prevent logging, auditing, testing, disclosure to oversight authorities, or other investigation necessary to enforce this section.

(4) Public-facing artificial intelligence communications.—Any Federal agency using artificial intelligence-generated content, synthetic media, digital persons, avatars, or automated interactive systems in communications with the public shall comply with sections 583 and 584.

(f) Narrow exception for individualized judicial warrant.—

(1) In general.—Subsection (b) shall not prohibit a use that is specifically authorized by a warrant issued by a court of competent jurisdiction upon probable cause, supported by oath or affirmation, and particularly describing the person or persons, place, account, device, or specific identifier to be surveilled and the artificial intelligence-enabled surveillance technique to be used.

(2) Strict construction.—The exception under paragraph (1) shall be construed narrowly and shall not authorize dragnet, population-scale, untargeted, or persistent surveillance of persons other than the person or persons specifically identified in the warrant.

(3) False statements or omissions.—Any officer, employee, or agent of the United States who knowingly or recklessly makes a materially false statement, or knowingly or recklessly omits material information, in an application for a warrant under this subsection shall be liable to the aggrieved person under section 1979 of the Revised Statutes ([42 U.S.C. 1983](#)), as amended by this Act, for appropriate relief, including actual damages, punitive damages where appropriate, declaratory relief, injunctive relief, and reasonable attorneys' fees and costs.

(4) No exigent circumstances exception.—A Federal agency may not invoke exigent circumstances to avoid the warrant requirement under this subsection.

(g) Logging, minimization, retention, and notice for permitted uses.—

(1) Logging.—Any use permitted under subsection (f) shall be subject to contemporaneous logging sufficient to identify the authorizing warrant, the persons with access, the data accessed, the outputs generated, and the actions taken in reliance on the system.

(2) Minimization.—Any use permitted under subsection (f) shall be conducted in a manner reasonably designed to minimize the collection, retention, access to, and use of data not

relevant to the purpose specifically authorized by the warrant, and the Federal agency shall retain and use only data reasonably necessary to carry out such purpose.

(3) Sensitive activities and privileged communications.—Any use permitted under subsection (f) shall be conducted under procedures reasonably designed to avoid, minimize, segregate, and restrict access to information concerning First Amendment activity, religious exercise, medical care, attorney-client communications, journalistic activity, lawful assembly, or other constitutionally protected or legally privileged activity that is not relevant to the purpose specifically authorized by the warrant.

(4) Retention and destruction.—

(A) Nonrelevant material.—Data, outputs, inferences, and derivative materials, including biometric probe images, biometric templates, candidate lists, match scores, and search outputs, obtained through a use permitted under subsection (f) that are not relevant to the purpose specifically authorized by the warrant shall be destroyed not later than 30 days after the end of the authorized surveillance period, unless a court orders continued retention for good cause shown.

(B) Relevant material.—Data, outputs, inferences, and derivative materials obtained through a use permitted under subsection (f) that are relevant to the purpose specifically authorized by the warrant may be retained only as required by the warrant, a court order, other applicable law, or evidentiary preservation obligations.

(5) Notice.—Within a reasonable time after the end of a surveillance period authorized under subsection (f), and not later than 30 days thereafter unless delayed by court order for good cause shown, the Federal agency shall provide notice to each person who was the target of surveillance under subsection (f) that such surveillance occurred.

(h) Suppression, exclusion, and invalidity of unlawfully obtained evidence.—

(1) In general.—No data, output, inference, lead, or evidence obtained or materially derived from a use in violation of this section may be received in evidence, relied upon, or otherwise used against any person in any trial, hearing, or other proceeding before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof.

(2) Fruit of the poisonous tree.—Any evidence derived from information obtained in violation of this section shall be subject to the same prohibition as the original information.

(i) Oversight, audits, and reports.—

(1) Interim final rules and guidance.—Not later than April 30, 2027, the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology and in consultation with the Director of the Office of Management and Budget, shall issue interim final rules and guidance to carry out this section. The interim final rules shall take effect upon publication in the Federal Register, shall have the force and effect of law, and may be issued without regard to [section 553 of title 5](#), United States Code. The Secretary shall provide a public comment period of not less than 60 days after publication and shall promulgate final rules not later than July 1, 2028.

(2) Inspector General audits.—The Inspector General of each Federal agency shall periodically audit compliance with this section and submit the results of such audit to Congress.

(3) Government Accountability Office review.—Not later than July 1, 2028, and biennially thereafter, the Comptroller General of the United States shall submit to Congress a report evaluating agency compliance with this section.

(4) Agency annual reports.—Not later than July 1 of each year, each Federal agency that used an exception under subsection (f) during the preceding year shall submit to Congress a report stating the number of warrant applications sought, granted, modified, or denied under this section and summarizing compliance with subsection (g).

(5) Public annual summary.—Not later than July 1 of each year, the Attorney General shall publish an annual public report summarizing Federal Government compliance with this section, including aggregate information concerning any uses permitted under subsection (f), except that classified or lawfully protected information may be withheld from the public version and provided in a classified annex to the appropriate congressional committees.

(j) Enforcement.—

(1) Civil actions by Attorney General.—Whenever the Attorney General has reason to believe that a Federal agency or any officer, employee, contractor, or agent thereof is engaged in a pattern or practice of violating this section, the Attorney General may bring a civil action in an appropriate district court of the United States for declaratory, injunctive, or other appropriate relief.

(2) Administrative discipline.—A knowing or willful violation of this section by an officer or employee of the United States shall be grounds for appropriate administrative discipline, including suspension or removal.

(3) No private right of action generally.—Except as provided in subsection (f)(3), nothing in this section shall be construed to create a private right of action.

(k) Whistleblower protection.—A disclosure of information evidencing a violation of this section shall be deemed a protected disclosure for purposes of section 588. Nothing in this subsection shall be construed to limit or displace any protection or remedy otherwise available under sections [2302\(b\)\(8\)](#) or [2303](#) of title 5, United States Code, [section 1034 of title 10](#), United States Code, or sections [3234](#) or [3341\(j\)](#) of title 50, United States Code, or to authorize the disclosure of classified information except through a channel authorized by law.

(l) Rule of construction.—Nothing in this section shall be construed to authorize any use of artificial intelligence that is otherwise prohibited by the Constitution or any other provision of law.

SEC. 1034. HIGH-IMPACT GOVERNMENT USE OF ARTIFICIAL INTELLIGENCE.

(a) Definitions.—In this section:

(1) Adverse AI incident.—The term "adverse AI incident" means any known or reasonably suspected event in which a high-impact artificial intelligence activity—

(A) materially enables, increases the risk of, or otherwise contributes to unlawful action, denial of rights, serious bodily injury, serious property damage, critical infrastructure disruption, cybersecurity compromise, or other severe public harm;

(B) materially enables, increases the risk of, or otherwise contributes to an adverse government action based on materially inaccurate, incomplete, or otherwise unreliable output or process;

(C) materially defeats, evades, or undermines any implemented safeguard;

(D) results in, or materially increases the risk of, unauthorized access to, disclosure of, exfiltration of, or material misuse of Government data or personal data processed by or through the activity; or

(E) materially enables autonomous cyber operations capable of causing substantial disruption to Government systems, critical infrastructure, or major economic activity.

(2) Artificial intelligence.—The term "artificial intelligence" has the meaning given that term in section 581.

(3) Federal agency.—The term "Federal agency" means an Executive agency, as defined in [section 105 of title 5](#), United States Code, and includes any military department.

(4) High-impact artificial intelligence activity.—The term "high-impact artificial intelligence activity" means the use, in whole or in part, by a Federal agency of any artificial intelligence system to make or materially inform a determination or action that may materially affect—

(A) the rights, liberties, safety, privacy, or property of any person;

(B) access to employment, education, housing, health care, credit, insurance, public accommodations, licenses, grants, contracts, benefits, or government services;

(C) immigration, border screening, detention, law enforcement, court administration or adjudication, criminal justice, military operations, intelligence activities, or national security activities;

(D) access to, or the security or operation of, critical infrastructure; or

(E) any other matter designated by the Secretary of Commerce, by regulation, as presenting a comparable risk of material harm.

(5) Impact assessment.—The term "impact assessment" means a written evaluation of the purpose, design, intended use, performance, limitations, data sources, cybersecurity, privacy risks, civil rights risks, error rates, foreseeable harms, and mitigation measures associated with a high-impact artificial intelligence activity.

(6) Meaningful human oversight.—The term "meaningful human oversight" means timely and informed human review, supervision, and authority over a high-impact artificial intelligence activity, including authority to interpret, question, disregard, override, or suspend the use of any artificial intelligence system used in such activity.

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

(8) Use case inventory.—The term "use case inventory" means a public or nonpublic catalog of high-impact artificial intelligence activities used by a Federal agency, including the function, legal authority, vendor, status, and risk designation of each such activity.

(b) Coverage and designation.—

(1) In general.—Each Federal agency shall identify and designate each high-impact artificial intelligence activity used or proposed to be used by the agency.

(2) Presumptive coverage.—An artificial intelligence activity shall be presumed to be a high-impact artificial intelligence activity if it is used or proposed to be used in any context described in subsection (a)(4)(A) through (D).

(3) Anti-evasion.—A Federal agency may not avoid designation under this subsection by characterizing an artificial intelligence activity as merely advisory, assistive, experimental, pilot, or nonfinal if such activity materially influences agency action.

(c) Governance requirements.—

(1) Responsible officials.—Each Federal agency using or proposing to use a high-impact artificial intelligence activity shall designate a senior responsible official to oversee compliance with this section.

(2) Internal governance.—Each such agency shall establish documented policies, procedures, and internal controls governing the approval, procurement, testing, deployment, monitoring, audit, material modification, suspension, and discontinuance of each high-impact artificial intelligence activity.

(3) Inventory and records.—Each such agency shall maintain a use case inventory and sufficient records to permit audit, oversight, and review of each high-impact artificial intelligence activity.

(d) Preconditions to procurement.—A Federal agency may not procure artificial intelligence for use in connection with a high-impact artificial intelligence activity unless, before such procurement—

(1) the agency has documented the legal authority for the intended use;

(2) the terms of use, technical design, and contractual restrictions applicable to the system do not prevent testing, logging, auditing, disclosure to oversight authorities, or other investigation necessary to enforce this section;

(3) the agency has established a process for independent review and meaningful human oversight of the activity; and

(4) the senior responsible official designated under subsection (c)(1) has approved the procurement in writing.

(e) Preconditions to deployment or use as a material basis for agency action.—A Federal agency may not deploy artificial intelligence in connection with a high-impact artificial intelligence

activity, or use the output of artificial intelligence as a material basis for a determination or action in connection with such an activity, unless, before such deployment or use—

- (1) the agency has completed an impact assessment;
 - (2) the agency has tested and validated the system for its intended use;
 - (3) the agency has established meaningful human oversight over the activity;
 - (4) the agency has adopted measures to identify and mitigate reasonably foreseeable risks to safety, privacy, civil rights, civil liberties, and due process;
 - (5) the agency has adopted measures reasonably designed to ensure that the activity functions reliably and universally across affected populations and to identify and mitigate systematic favoritism or disfavor toward any subset of such population;
 - (6) the agency has established logging, auditability, incident reporting, and record retention procedures sufficient to permit review of the activity and its outputs;
 - (7) the agency has completed an independent review of the activity by appropriate officials who are not part of the sponsoring program office, including officials responsible for legal compliance, privacy, civil rights or civil liberties, cybersecurity, and records management, as applicable;
 - (8) if the activity is a new externally facing high-impact artificial intelligence activity, and except to the extent expressly prohibited by law or impracticable in classified, military, intelligence, national security, or law enforcement operations, the agency has published a plain language summary of the impact assessment and provided not fewer than 30 days for public comment before initial deployment; and
 - (9) the senior responsible official designated under subsection (c)(1) has approved the deployment or use in writing.
- (f) Required safeguards.—Each Federal agency engaging in a high-impact artificial intelligence activity shall—

- (1) ensure that the activity is used only for a documented and lawful purpose;
- (2) conduct predeployment testing, red team testing where appropriate, and periodic reevaluation of system performance, limitations, and failure modes;
- (3) assess and mitigate reasonably foreseeable risks of bias, discrimination, privacy invasion, unlawful surveillance, security compromise, hallucination, inaccuracy, and harmful overreliance;
- (4) maintain technical and organizational safeguards sufficient to protect Government data and any personal data processed by or through the activity;
- (5) provide meaningful human oversight over any agency action materially informed by the activity;

(6) provide, before any final materially adverse agency action materially informed by the activity, to any person materially adversely affected by such action, except to the extent expressly prohibited by law or impracticable in classified or military operations—

(A) notice that artificial intelligence was used;

(B) a description of the role that the activity played in the action;

(C) notice of the principal categories of data materially relied upon, to the extent consistent with law and the protection of classified, privileged, or otherwise protected information; and

(D) an opportunity for review, correction, contest, or appeal before an official with authority to disregard or reverse the output of the activity;

(7) ensure that no final adverse agency action is based solely on the output of artificial intelligence used in the activity; and

(8) suspend or discontinue use of the system when the agency cannot reasonably mitigate material risks associated with the high-impact artificial intelligence activity.

(g) Transition for existing activities.—

(1) Existing activity defined.—In this subsection, the term "existing activity" means a high-impact artificial intelligence activity used by a Federal agency on the date of enactment of this Act.

(2) Inventory and provisional approval.—Not later than 90 days after the date of enactment of this Act, each Federal agency shall—

(A) identify each existing activity;

(B) enter the activity in the use case inventory maintained under subsection (c)(3); and

(C) obtain written provisional approval for continued use from the senior responsible official designated under subsection (c)(1).

(3) Contents of provisional approval.—A provisional approval under paragraph (2) shall document the legal authority and operational necessity for the existing activity, its principal known or reasonably foreseeable risks, and the interim safeguards governing its continued use.

(4) Continued use during transition.—Notwithstanding subsection (e), a Federal agency may continue an existing activity until the compliance deadline under paragraph (5), and may satisfy the testing requirement under subsection (f)(2) during that period rather than before deployment, only while—

(A) a provisional approval under paragraph (2) remains in effect; and

(B) the agency maintains meaningful human oversight, logging, incident reporting, and safeguards reasonably designed to identify and mitigate material risks.

(5) Compliance deadline.—Not later than 180 days after publication of the interim final rules under subsection (k)(1), each Federal agency shall complete the requirements of subsection (e) with respect to each existing activity and approve, modify, suspend, or discontinue the activity.

(6) Inventory status.—For purposes of subsection (i)(2)(E), an existing activity operating under a valid provisional approval shall be identified as operating under the transition authorized by this subsection and shall not be described as noncompliant solely because the impact assessment required under subsection (e)(1) has not been completed.

(7) Prior procurements.—Subsection (d) shall not apply to a procurement completed before the date of enactment of this Act, but shall apply to a renewal, extension, replacement, material modification, or new procurement occurring on or after that date.

(8) Immediate safeguards.—Nothing in this subsection shall—

(A) authorize an activity prohibited under section 1033; or

(B) delay the application of the suspension and discontinuance requirements under subsection (j)(6) and (7).

(h) Material changes.—A Federal agency may not materially expand or materially alter a high-impact artificial intelligence activity without completing a supplemental impact assessment and obtaining updated written approval under subsection (e)(9).

(i) Transparency and inventory.—

(1) Public inventory.—Each Federal agency shall publish and maintain a publicly accessible inventory of high-impact artificial intelligence activities used by the agency.

(2) Contents.—The inventory required under paragraph (1) shall include, for each listed activity—

(A) a general description of the activity and its purpose;

(B) the vendor or developer, if any;

(C) the legal authority for use;

(D) the date the activity was first deployed;

(E) a short summary of the impact assessment required under this section, including the principal risks identified and the principal safeguards or mitigation measures adopted by the agency, or, if the impact assessment has not been completed, a statement that the activity is not in compliance with this section; and

(F) such additional information as the Secretary of Commerce, acting through the Director of the National Institute of Standards and Technology, may require by regulation or guidance.

(3) Exceptions.—A Federal agency may withhold or redact information from the public inventory only to the extent necessary to protect classified information, law enforcement

sensitivity, operational security, or other interests protected by law, but shall maintain a complete nonpublic inventory available for oversight.

(j) Monitoring, incident reporting, suspension, and discontinuance.—

(1) Ongoing monitoring.—Each Federal agency shall continuously monitor the performance and impacts of each high-impact artificial intelligence activity used by the agency.

(2) Initial incident reporting.—A Federal agency shall report an adverse AI incident not later than 72 hours after discovery, or as soon thereafter as practicable if the agency demonstrates good cause for delay, to—

(A) the Secretary, acting through the Director of the National Institute of Standards and Technology;

(B) the Inspector General of the Federal agency; and

(C) the Attorney General, if the incident appears to involve unlawful conduct or a material risk to civil rights, civil liberties, or due process.

(3) Contents of initial report.—An initial report under paragraph (2) shall include, to the extent known at the time of submission—

(A) the identity of the reporting Federal agency;

(B) a description of the high-impact artificial intelligence activity involved;

(C) the date of discovery and the known or reasonably suspected date or period of occurrence;

(D) the nature of the adverse AI incident;

(E) the known or reasonably suspected harms or risks arising from the incident;

(F) whether the activity has been suspended, limited, modified, or discontinued;

(G) any immediate mitigation measures taken; and

(H) such other information as the Secretary may require by regulation.

(4) Supplemental reports.—A Federal agency that submits an initial report under paragraph (2) shall submit supplemental reports at such times and in such form as the Secretary may require by regulation, including when—

(A) material new facts become known;

(B) the agency determines that an affected activity should be suspended, modified, resumed, or discontinued;

(C) the agency determines that notice should be provided to affected persons under this section; or

(D) the agency completes a material part of its investigation or remediation.

(5) Incident response and preservation duties.—Upon discovering an adverse AI incident, a Federal agency shall—

(A) take reasonable measures to contain, mitigate, and document the incident;

(B) preserve records, logs, outputs, model settings, prompts, instructions, data inputs, decision records, and other materials reasonably necessary to investigate the incident and assess compliance with this section; and

(C) determine whether the high-impact artificial intelligence activity should be suspended, modified, or discontinued, and whether any materially affected person should receive notice, review, correction, contest, or appeal rights under this section.

(6) Suspension.—A Federal agency shall promptly suspend use of a high-impact artificial intelligence activity upon determining that the activity presents a substantial and unmitigated risk of unlawful action, material inaccuracy, material security failure, or material harm to safety, privacy, civil rights, or civil liberties.

(7) Discontinuance.—A Federal agency shall discontinue use of a high-impact artificial intelligence activity when the agency determines that compliance with this section cannot reasonably be achieved.

(k) Oversight and enforcement.—

(1) Regulations and guidance.—Not later than April 30, 2027, the Secretary, acting through the Director of the National Institute of Standards and Technology and in consultation with the Attorney General, shall promulgate interim final rules and guidance to carry out this section. The interim final rules shall take effect upon publication in the Federal Register, shall have the force and effect of law, and may be issued without regard to [section 553 of title 5](#), United States Code. The Secretary shall provide a public comment period of not less than 60 days after publication and shall promulgate final rules not later than July 1, 2028.

(2) Interagency coordination.—The Secretary, acting through the Director of the National Institute of Standards and Technology, shall convene an interagency council of representatives designated by Federal agencies subject to this section to promote consistent implementation, share best practices, identify common risks, and develop recommendations for guidance and updates under paragraph (1).

(3) Inspector General review.—The Inspector General of each Federal agency using a high-impact artificial intelligence activity shall periodically audit compliance with this section and submit the results of such audit to Congress.

(4) Government Accountability Office review.—Not later than July 1, 2028, and biennially thereafter, the Comptroller General of the United States shall submit to Congress a report evaluating agency compliance with this section.

(l) Rule of construction.—Nothing in this section shall be construed—

(1) to authorize any use of artificial intelligence prohibited under section 1033; or

(2) to authorize any use of artificial intelligence otherwise prohibited by the Constitution or any other provision of law.

SEC. 1035. ARTIFICIAL INTELLIGENCE PROCUREMENT.

(a) Definitions.—In this section:

(1) Artificial intelligence.—The term "artificial intelligence" has the meaning given that term in section 581.

(2) Cloud computing.—The term "cloud computing" has the meaning given that term in Special Publication 800–145 of the National Institute of Standards and Technology, or any successor document.

(3) Data infrastructure.—The term "data infrastructure" means the underlying computer, network, and software systems that enable the collection, storage, processing, and analysis of data, including the ability to record, transmit, transform, categorize, integrate, and otherwise process data generated by digital data systems.

(4) Digital solution.—The term "digital solution" means any cloud computing service, data infrastructure, foundation model, or other artificial intelligence product or service procured, licensed, subscribed to, accessed, or used by a Federal agency.

(5) Federal agency.—The term "Federal agency" means an Executive agency, as defined in [section 105 of title 5](#), United States Code, and includes any military department.

(6) Foundation model.—The term "foundation model" means an artificial intelligence model that—

(A)—

(i) generally uses self-supervision;

(ii) contains at least 1,000,000,000 parameters; and

(iii) is applicable across a wide range of contexts; or

(B) exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health, or safety.

(7) Government-furnished data.—The term "Government-furnished data" means data, and any associated metadata, logs, configurations, prompts, outputs, or derivative records, provided by or generated for or on behalf of a Federal agency through the development, testing, deployment, operation, or use of a digital solution.

(8) Multi-cloud technology.—The term "multi-cloud technology" means architecture and services that allow for data, application, and program portability, usability, and interoperability between infrastructure, platforms, and hosted applications of multiple cloud providers and between public, private, and edge cloud environments in a manner that securely delivers operational and management consistency, comprehensive visibility, and resiliency.

(b) Government-wide procurement requirements.—The head of each Federal agency, and the Administrator of General Services with respect to any Government-wide acquisition vehicle, shall ensure that each procurement of a digital solution—

(1) uses a competitive award process unless another provision of law expressly authorizes a noncompetitive procurement and the head of the Federal agency makes a written determination justifying the use of such authority;

(2) preserves for the Federal Government exclusive rights to access and use all Government-furnished data, except to the extent that rights in preexisting vendor materials are expressly reserved by contract and do not impair Government access and use;

(3) prioritizes the appropriate allocation of intellectual property and data rights to protect Government access, use, portability, security, interoperability, and auditability;

(4) includes modular open systems approaches and appropriate work allocation and technical boundaries;

(5) uses open, documented, externally accessible, machine-readable interfaces using industry standard, nonproprietary technologies, protocols, and payloads where feasible;

(6) provides for storage and management of Government-furnished data in a provider-agnostic and environment-agnostic manner, uncoupled from unnecessary hardware or software dependencies;

(7) provides for portability and exportability of Government-furnished data in a usable format and without unreasonable cost or delay;

(8) prioritizes multi-cloud technology where feasible and advantageous;

(9) mitigates barriers to entry faced by small business concerns and nontraditional contractors;

(10) prohibits pricing structures, introductory offers, trial terms, contractual restrictions, or technical design choices that create unreasonable vendor lock-in or materially impair transition to another provider;

(11) requires the procuring Federal agency to assess and document reasonably anticipated lifecycle costs, switching costs, usage-based cost escalation, and exit costs before award;

(12) if the procurement involves no-cost, nominal-cost, or introductory-price access to a digital solution, requires a written determination by the head of the Federal agency that the agency has evaluated lifecycle costs, usage-based cost growth, switching costs, exit costs, and data portability before accepting such access; and

(13) includes requirements sufficient to permit Government inspection, testing, logging, auditing, post-award monitoring, and oversight of security, performance, costs, and compliance.

(c) Government data and training protections.—Not later than April 30, 2027, the Federal Acquisition Regulatory Council shall amend the Federal Acquisition Regulation to ensure that each contract for a digital solution provides that—

(1) Government-furnished data may not be disclosed, retained, transferred, licensed, sold, or used without proper authorization by the relevant Federal agency;

(2) Government-furnished data stored on vendor systems are segregated from other data on such systems and protected through reasonable administrative, technical, and physical safeguards;

(3) Government-furnished data may not be used to train, fine-tune, retrain, evaluate, or otherwise improve any artificial intelligence product or service except as expressly authorized by the relevant Federal agency;

(4) the relevant Federal agency is able, upon request and without unreasonable cost or delay, to retrieve and export Government-furnished data in a usable format;

(5) violation of the contract provisions required under this subsection shall be subject to specific penalties, including fines, contract termination, and such other contractual remedies as the head of the relevant Federal agency determines appropriate; and

(6) no contractor may satisfy a contractual requirement for security, compliance, or performance review solely through an assessment, audit, attestation, or similar review paid for by the contractor or an affiliate of the contractor.

(d) Additional Department of Defense implementation.—

(1) In general.—Not later than April 30, 2027, the Secretary of Defense shall direct the Chief Digital and Artificial Intelligence Office and the Under Secretary of Defense for Acquisition and Sustainment to update or promulgate provisions of the Defense Federal Acquisition Regulation Supplement to implement this section for the Department of Defense.

(2) Exemptions.—A component acquisition executive may issue an exemption from a requirement of this section only upon—

(A) determining in writing that issuing the exemption is not inconsistent with national security;

(B) identifying the specific requirement exempted, the vendor and program receiving the exemption, and the justification for the exemption; and

(C) notifying the Chief Digital and Artificial Intelligence Officer of the exemption.

(e) Noncompliant procurement terms.—A Federal agency may not award, renew, extend, or exercise an option under a contract for a digital solution if the solicitation, contract, renewal, extension, or option materially fails to comply with subsection (b), unless the head of the Federal agency determines in writing that exigent circumstances require continued performance for a period not to exceed 180 days and submits the determination to the Administrator of General Services and the Inspector General of the Federal agency.

(f) Rule of construction.—Nothing in this section shall be construed to limit any stronger restriction, safeguard, or prohibition applicable under this subtitle or any other provision of law.

SEC. 1036. CENTER FOR AI STANDARDS AND INNOVATION.

(a) Definitions.—In this section:

(1) CAISI.—The term "CAISI" means the Center for AI Standards and Innovation established under subsection (b).

(2) Digital solution.—The term "digital solution" has the meaning given that term in section 1035.

(3) Federal agency.—The term "Federal agency" means an Executive agency, as defined in [section 105 of title 5](#), United States Code, and includes any military department.

(4) NIST.—The term "NIST" means the National Institute of Standards and Technology.

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

(b) Establishment.—There is established within NIST the Center for AI Standards and Innovation.

(c) Duties of CAISI.—The Secretary, acting through CAISI, shall—

(1) develop, publish, and periodically update guidelines, best practices, evaluation methods, benchmarks, and tools supporting voluntary standards relating to the security, reliability, and functionality of artificial intelligence systems;

(2) conduct and support unclassified evaluations of artificial intelligence capabilities that may pose material risks to public safety, national security, critical infrastructure, cybersecurity, biosecurity, or chemical weapons security;

(3) evaluate and assess security vulnerabilities and malign foreign influence risks arising from the use of artificial intelligence systems developed in the United States or abroad;

(4) support Federal agencies in the evaluation of artificial intelligence systems proposed to be used in Government operations and procurement, including through collaboration with the General Services Administration and other agencies responsible for acquisition and shared services;

(5) coordinate with Federal agencies, including the Department of Defense, the Department of Energy, the Department of Homeland Security, the Office of Science and Technology Policy, and the intelligence community, as appropriate, to develop evaluation methods, share technical expertise, and support secure and interoperable adoption of artificial intelligence;

(6) support the development of voluntary, consensus-based, and interoperable standards for artificial intelligence systems and related provenance, labeling, evaluation, and security practices;

(7) provide technical assistance and measurement science support for the implementation of sections 1033 through 1035 and subtitle F of title V; and

(8) submit to Congress the reports required under subsection (g).

(d) Government-wide procurement review capability.—

(1) In general.—The Administrator of General Services, acting through the Federal Risk and Authorization Management Program and in consultation with the Secretary, acting through CAISI, the Director of the Cybersecurity and Infrastructure Security Agency, and the Administrator for Federal Procurement Policy, shall establish and maintain a Government-wide capability to perform or commission independent technical review of digital solutions used or proposed to be used by Federal agencies for purposes of procurement and acquisition oversight.

(2) Scope.—The capability required under paragraph (1) shall be limited to review of procurement-facing risks and requirements associated with digital solutions, including—

- (A) cybersecurity;
- (B) auditability and logging;
- (C) Government data rights;
- (D) portability and exportability;
- (E) interoperability and multi-cloud compatibility;
- (F) lifecycle costs, switching costs, and vendor lock-in risks; and
- (G) conflicts of interest in third-party assessment.

(3) Rule of construction.—Nothing in this subsection shall be construed to authorize the Administrator of General Services, the Federal Risk and Authorization Management Program, or CAISI to make a final determination regarding the substantive legality, mission appropriateness, or programmatic permissibility of an agency use of artificial intelligence, which determinations shall remain with the procuring Federal agency subject to applicable law.

(e) Standards, guidance, and interagency support.—Not later than April 30, 2027, the Secretary, acting through CAISI, and the Administrator of General Services, acting through the Federal Risk and Authorization Management Program, shall jointly issue such standards and guidance as are necessary to carry out subsection (d) and subsection (f), including standards and guidance relating to evaluation integrity, procurement-facing artificial intelligence risks, and the avoidance of unreasonable vendor lock-in.

(f) Evaluation integrity and anti-capture.—In carrying out this section, the Secretary, the Administrator of General Services, CAISI, and the Federal Risk and Authorization Management Program shall—

(1) require disclosure of any material financial, contractual, employment, or organizational conflict of interest affecting an evaluation, assessment, benchmark, review, or procurement-facing technical analysis under this section;

(2) ensure that no evaluation, assessment, benchmark, review, or procurement-facing technical analysis under this section is controlled by a person with a material financial interest in the vendor, contractor, model, system, or digital solution being evaluated;

(3) ensure that no Federal agency relies solely on an assessment, audit, attestation, certification, benchmark, or similar review paid for or controlled by the vendor or an affiliate of the vendor to satisfy a requirement under this section;

(4) publish evaluation methods, benchmark descriptions, conformity profiles, and review criteria to the greatest extent practicable, consistent with national security, cybersecurity, trade secret protection, and other applicable law; and

(5) ensure that standards, benchmarks, reviews, and procurement-facing technical analyses under this section do not unnecessarily favor dominant vendors, proprietary architectures, closed interfaces, or noninteroperable systems over smaller vendors, open standards, interoperable systems, or nonproprietary alternatives.

(g) Reports.—

(1) CAISI report.—Not later than July 1, 2027, and annually thereafter for 4 years, the Secretary, acting through CAISI, shall submit to Congress a report describing—

(A) the activities carried out under subsection (c);

(B) significant findings from evaluations, assessments, and standards work conducted under this section, including any recurring security or functionality concerns;

(C) recommendations for legislative and administrative action; and

(D) the resources, staffing, and appropriations needed to carry out this section.

(2) Procurement review report.—Not later than July 1, 2027, and annually thereafter for 4 years, the Administrator of General Services, in consultation with the officials specified in subsection (d)(1) and the heads of relevant Federal agencies, shall submit to Congress a report assessing competition, innovation, barriers to entry, switching costs, vendor lock-in risks, reliance on vendor-paid assessments, and concentrations of market power or market share in the artificial intelligence, cloud computing, data infrastructure, and foundation model space for each period covered by the report, together with recommendations for legislative and administrative action.

(3) Defense supplement.—Each procurement review report shall include a supplement prepared by the Secretary of Defense describing implementation of section 1035(d) by the Department of Defense, including exemptions granted under section 1035(d)(2).

(4) Publication.—The Administrator of General Services shall ensure that a publicly releasable version of each procurement review report is made available on appropriate websites.

(h) Authorization of appropriations.—

(1) CAISI and NIST support.—There are authorized to be appropriated to the Secretary, acting through NIST and CAISI, such sums as may be necessary for each of fiscal years 2027 through 2031 to carry out this section.

(2) Procurement review capacity.—There are authorized to be appropriated to the Administrator of General Services, acting through the Federal Risk and Authorization Management Program, \$30,000,000 for each of fiscal years 2027 through 2031 to carry out subsection (d), including staffing, technical analysis, independent testing, conflict-of-interest screening, and other support necessary to maintain the capability required under such subsection.

(i) Rule of construction.—Nothing in this section shall be construed to limit or displace any stronger restriction, safeguard, or prohibition applicable under section 1033, section 1034, section 1035, subtitle F of title V, or any other provision of law.

Subtitle D—Government Transparency and Improved Rulemaking

SEC. 1041. AMENDMENT TO THE FREEDOM OF INFORMATION ACT.

(a) Amendments to section 552(a).—[Section 552\(a\) of title 5](#), United States Code (commonly known as the "Freedom of Information Act") is amended—

(1) in paragraph (2)—

(A) in subparagraph (D)(i)(II), by striking "and";

(B) in subparagraph (E), by adding after the semicolon the following: "and

"(F) (i) materials related to the operations and establishment of advisory committees (as defined in section 1001) and any subcommittee thereof, including events, timelines, agendas, minutes, transcripts, recordings, committee member names and biographies, conflict of interest waivers, committee charters, and any other related materials;

"(ii) unclassified reports submitted to Congress by the head of the agency;

"(iii) unclassified testimony submitted to Congress by the head of the agency;

"(iv) agency organization charts and directories with the contact information for all offices of the agency;

"(v) any log relating to a request for a record under paragraph (3), including any tracking number assigned to the request, the date the request was received by the head of the agency, the subject of the request, and the disposition of the request;

"(vi) any record that reflects the official calendar of the head of the agency, including a record that reflects an event, meeting, or telephone call scheduled for the head of the agency;

"(vii) a list—

"(I) identifying—

"(aa) each contract or grant of the agency with a value exceeding \$100,000,000; or