118th CONGRESS

2nd Session

H.R. 8847

COMPREHENSIVE NATIONAL INFRASTRUCTURE MODERNIZATION, DIGITAL TRANSFORMATION, ARTIFICIAL INTELLIGENCE GOVERNANCE, CYBERSECURITY ENHANCEMENT, AND SUSTAINABLE TECHNOLOGY DEVELOPMENT ACT OF 2024

[The CNIMDT-AIGCE-STD Act]

IN THE HOUSE OF REPRESENTATIVES

March 15, 2024

Mr. RICHARDSON of California (for himself, Ms. CHEN of New York, Mr. BLACKWOOD of Texas, Mrs. OKONKWO of Illinois, Mr. PETERSEN of Florida, Ms. YAMAMOTO of Washington, Mr. KOWALSKI of Michigan, Mrs. JEFFERSON of Georgia, Mr. SINGH of New Jersey, and Ms. O'BRIEN of Massachusetts) introduced the following bill; which was referred to the Committee on Energy and Commerce, the Committee on Science, Space, and Technology, the Committee on Homeland Security, the Committee on Ways and Means, the Committee on Transportation and Infrastructure, and the Committee on Financial Services

A BILL

To establish a comprehensive national framework for the modernization of critical infrastructure, the governance of artificial intelligence systems, the enhancement of cybersecurity capabilities, the development of sustainable technology initiatives, the protection of digital rights and privacy, the promotion of technological innovation and competitiveness, the creation of workforce development programs for emerging technologies, the establishment of public-private partnerships for research and development, and for other purposes.

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

TABLE OF CONTENTS

TITLE I - GENERAL PROVISIONS AND DEFINITIONS

CHAPTER 1 - SHORT TITLE AND FINDINGS

SEC. 101. SHORT TITLE.

(a) SHORT TITLE.—This Act may be cited as the 'Comprehensive National Infrastructure Modernization, Digital Transformation, Artificial Intelligence Governance, Cybersecurity Enhancement, and Sustainable Technology Development Act of 2024' or the 'CNIMDT-AIGCE-STD Act'.

(b) TABLE OF CONTENTS.—The table of contents for this Act is set forth in the preceding pages.

SEC. 102. FINDINGS.

Congress finds the following:

(1) The United States faces unprecedented challenges and opportunities arising from rapid technological advancement, including the proliferation of artificial intelligence systems, increasing cybersecurity threats, aging physical and digital infrastructure, and the urgent need to transition to sustainable technologies.

(2) Critical infrastructure in the United States, including transportation networks, energy systems, water treatment facilities, telecommunications networks, and digital platforms, requires significant modernization to meet the demands of the 21st century economy and to ensure national security.

(3) Artificial intelligence technologies present transformative opportunities for economic growth, scientific advancement, and improved quality of life, while simultaneously raising significant concerns regarding safety, transparency, accountability, bias, privacy, and potential displacement of workers.

(4) The Nation's cybersecurity posture must be strengthened to protect against increasingly sophisticated threats from nation-state actors, criminal organizations, terrorist groups, and other malicious entities targeting critical infrastructure, government systems, private enterprises, and individual citizens.

(5) Digital technologies have become integral to daily life in the United States, necessitating comprehensive frameworks to protect individual privacy rights, ensure algorithmic fairness, prevent discrimination, and safeguard democratic institutions from technological manipulation.

(6) The development and deployment of new technologies must be guided by principles of environmental sustainability, recognizing the significant carbon footprint of digital infrastructure and the potential for technology to either exacerbate or mitigate climate change impacts.

(7) Maintaining the technological competitiveness of the United States requires sustained investment in research and development, effective technology transfer mechanisms, robust intellectual property protections, and strategic international partnerships.

(8) The rapid pace of technological change necessitates comprehensive workforce development programs to ensure that American workers have the skills necessary to participate in the digital economy and that displaced workers receive adequate support and retraining opportunities.

(9) Effective governance of emerging technologies requires coordination among Federal agencies, State and local governments, the private sector, academic institutions, civil society organizations, and international partners.

(10) Previous legislative efforts addressing individual aspects of technology policy have resulted in a fragmented regulatory landscape that imposes unnecessary burdens on businesses, creates uncertainty for consumers, and fails to adequately address cross-cutting issues.

(11) A comprehensive, integrated approach to technology policy is necessary to ensure that the United States remains at the forefront of technological innovation while protecting the rights, safety, and

well-being of its citizens.

(12) Small and medium-sized enterprises require particular attention and support in adapting to new technological requirements and opportunities, as they constitute the backbone of the American economy and are often most affected by regulatory changes.

(13) Rural and underserved communities have historically been left behind in technological advancement, exacerbating existing inequalities and limiting economic opportunities for millions of Americans.

(14) The protection of children in digital environments requires special consideration, given their unique vulnerabilities to online harms, data exploitation, and algorithmic manipulation.

(15) International coordination on technology governance is essential, as technologies operate across national boundaries and unilateral approaches may be insufficient to address global challenges.

SEC. 103. PURPOSES.

The purposes of this Act are—

(1) to establish a comprehensive national framework for the governance of emerging technologies, including artificial intelligence, that balances innovation with appropriate safeguards for safety, transparency, accountability, and human rights;

(2) to modernize critical infrastructure across all sectors, including transportation, energy, water, telecommunications, and digital systems, to ensure resilience, efficiency, and sustainability;

(3) to enhance the cybersecurity posture of the Nation through improved threat detection, incident response capabilities, information sharing mechanisms, and workforce development;

(4) to protect the digital rights and privacy of individuals, including protections against algorithmic discrimination, data exploitation, and technological manipulation;

(5) to promote the development and deployment of sustainable technologies that reduce environmental impacts, support climate goals, and advance principles of circular economy;

(6) to strengthen the technological competitiveness of the United States through strategic investments in research and development, technology transfer, and international cooperation;

(7) to develop a workforce equipped with the skills necessary to thrive in the digital economy, with particular attention to displaced workers, underserved communities, and emerging fields;

(8) to establish clear, consistent, and effective enforcement mechanisms that promote compliance while avoiding unnecessary burdens on innovation and economic growth;

(9) to ensure that the benefits of technological advancement are broadly shared across society, including in rural and underserved communities;

(10) to protect children from online harms while preserving their ability to benefit from digital technologies for education, creativity, and social connection.

SEC. 104. POLICY PRINCIPLES.

(a) IN GENERAL.—It is the policy of the United States that the governance of emerging technologies shall be guided by the following principles:

(1) HUMAN-CENTERED DESIGN.—Technologies should be designed and deployed to enhance human capabilities, respect human dignity, and serve human needs, with human oversight maintained over consequential decisions.

(2) SAFETY AND SECURITY.—Technologies should be developed with robust safety measures, thoroughly tested for potential harms, and continuously monitored for emerging risks throughout their lifecycle.

(3) TRANSPARENCY AND EXPLAINABILITY.—The functioning of technological systems, particularly those making consequential decisions affecting individuals or communities, should be transparent and explainable to affected parties.

(4) ACCOUNTABILITY.—Clear lines of accountability should exist for the development, deployment, and outcomes of technological systems, with appropriate mechanisms for redress when harms occur.

(5) FAIRNESS AND NON-DISCRIMINATION.—Technologies should be designed and deployed to prevent discrimination and ensure equitable outcomes across different demographic groups.

(6) PRIVACY AND DATA PROTECTION.—Individual privacy rights should be protected through meaningful consent mechanisms, data minimization practices, and robust security measures.

(7) INNOVATION AND COMPETITIVENESS.—Regulatory frameworks should support American innovation and global competitiveness while ensuring appropriate safeguards are in place.

(8) ENVIRONMENTAL SUSTAINABILITY.—Technology development should minimize environmental impacts, support climate goals, and advance principles of sustainable design.

(9) INTEROPERABILITY AND STANDARDS.—Technologies should be developed with attention to interoperability, open standards, and portability to prevent lock-in and promote competition.

(10) DEMOCRATIC VALUES.—Technology governance should protect democratic institutions, support informed public discourse, and preserve individual freedoms.

(b) APPLICATION.—The principles set forth in subsection (a) shall guide the interpretation and implementation of this Act and any regulations promulgated thereunder.

CHAPTER 2 - DEFINITIONS

SEC. 110. DEFINITIONS.

In this Act, unless otherwise specified:

(1) ADMINISTRATOR.—The term 'Administrator' means the Administrator of the National Technology Governance Administration established under section 901 of this Act.

(2) ADVANCED COMPUTING.—The term 'advanced computing' means computing technologies that significantly exceed conventional capabilities, including but not limited to quantum computing, neuromorphic computing, and high-performance computing systems capable of performing more than 10 to the power of 18 floating-point operations per second.

(3) ADVERSE ACTION.—The term 'adverse action' means, with respect to an individual, any action that materially harms that individual's interests, including but not limited to denial of credit, insurance, housing, employment, education, or government benefits; arrest, detention, or criminal prosecution; imposition of civil penalties or sanctions; or denial of access to essential services or public accommodations.

(4) AGENCY.—The term 'agency' has the meaning given such term in section 551 of title 5, United States Code, except that such term does not include the Government Accountability Office, the Board of Governors of the Federal Reserve System, or an entity described in section 552(f) of such title.

(5) ALGORITHMIC DECISION SYSTEM.—The term 'algorithmic decision system' means any computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes or materially supports a decision or facilitates human decision making regarding persons.

(6) ALGORITHMIC IMPACT ASSESSMENT.—The term 'algorithmic impact assessment' means a documented evaluation of an algorithmic decision system, conducted prior to deployment and periodically thereafter, that assesses potential impacts on the rights, safety, and well-being of affected individuals and communities, including analysis of accuracy, fairness, privacy, security, and

transparency.

(7) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means the Committee on Energy and Commerce, the Committee on Science, Space, and Technology, and the Committee on Homeland Security of the House of Representatives, and the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate.

(8) ARTIFICIAL GENERAL INTELLIGENCE.—The term 'artificial general intelligence' or 'AGI' means an artificial intelligence system that can perform intellectual tasks across a wide range of domains with capabilities that meet or exceed those of a human adult, including the ability to learn new skills, reason abstractly, plan strategically, and transfer knowledge across domains without task-specific training.

(9) ARTIFICIAL INTELLIGENCE.—The term 'artificial intelligence' or 'AI' means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

(10) BIOMETRIC DATA.—The term 'biometric data' means data generated by automatic measurements of an individual's biological characteristics, including fingerprints, voice prints, iris or retina scans, face prints, hand prints, palm prints, vein patterns, gait patterns, and any other biological characteristic that can be used to establish individual identity.

(11) BROADBAND INTERNET ACCESS SERVICE.—The term 'broadband internet access service' means a mass-market retail service by wire or radio that provides the capability to transmit data to and receive data from all or substantially all internet endpoints, including any capabilities that are incidental to and enable the operation of the communications service, but excluding dial-up internet access service.

(12) CHILD.—The term 'child' means an individual who has not attained the age of 13 years.

(13) COMMISSION.—The term 'Commission' means the Federal Trade Commission.

(14) CONSENT.—The term 'consent' means a clear affirmative act by an individual that is freely given, specific, informed, and unambiguous, indicating that individual's agreement to the processing of personal data relating to him or her. Consent obtained through dark patterns, deceptive design, or coercion shall not constitute valid consent for purposes of this Act.

(15) CONSEQUENTIAL DECISION.—The term 'consequential decision' means a decision or judgment that has a legal, material, or similarly significant effect on an individual's life relating to access to or the cost, terms, or conditions of: (A) employment or employment opportunities; (B) education or educational opportunities; (C) housing or lodging; (D) credit or insurance; (E) healthcare or healthcare services; (F) public benefits or government services; (G) access to essential services or utilities; (H) criminal justice, including policing, bail, sentencing, and parole; or (I) other essential services, opportunities, or outcomes as determined by the Administrator through rulemaking.

(16) CONTROLLER.—The term 'controller' means an entity that, alone or jointly with others, determines the purposes and means of the processing of personal data.

(17) COVERED ALGORITHM.—The term 'covered algorithm' means any computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes or materially supports a consequential decision.

(18) COVERED ENTITY.—The term 'covered entity' means any person or entity that: (A) is subject to the jurisdiction of the Commission under section 5 of the Federal Trade Commission Act (15 U.S.C. 45); (B) is a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); (C) is a nonprofit organization described in section 501(c) of the Internal Revenue Code of 1986; or (D) operates within the United States or processes the personal data of individuals located within the United States.

(19) COVERED PLATFORM.—The term 'covered platform' means an online platform that: (A) has at least 50,000,000 monthly active users of a product or service in the United States; (B) is owned or controlled by a person with annual gross revenues in excess of $25,000,000,000; or (C) has at least 1,000,000,000 monthly active users worldwide of any product or service.

(20) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given that term in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)) and includes: (A) chemical facilities; (B) commercial facilities; (C) communications networks; (D) critical manufacturing; (E) dams; (F) defense industrial base; (G) emergency services; (H) energy systems; (I) financial services; (J) food and agriculture; (K) government facilities; (L) healthcare and public health; (M) information technology; (N) nuclear reactors, materials, and waste; (O) transportation systems; (P) water and wastewater systems; and (Q) space systems.

(21) CYBERSECURITY INCIDENT.—The term 'cybersecurity incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

(22) DARK PATTERN.—The term 'dark pattern' means a user interface or design feature that has the effect of substantially subverting or impairing user autonomy, decision making, or choice, including features that: (A) are designed to induce deceptive, manipulative, or confusing user interface or behavior; (B) employ confusing language or interactive features; (C) take advantage of user inattention or cognitive biases; or (D) manipulate user emotions.

(23) DATA BROKER.—The term 'data broker' means a commercial entity that collects, assembles, or maintains personal data concerning an individual who is not a customer or an employee of that entity in order to sell or otherwise provide such data to another entity or to analyze such data for another entity.

(24) DATA MINIMIZATION.—The term 'data minimization' means the limitation of the collection, processing, and retention of personal data to what is directly relevant and necessary to accomplish a specified purpose.

(25) DE-IDENTIFIED DATA.—The term 'de-identified data' means data that cannot reasonably be used to infer information about, or otherwise be linked to, an identified or identifiable individual, or a device linked to such individual, if the covered entity that possesses such data: (A) takes reasonable technical measures to ensure that the data cannot be associated with an individual; (B) publicly commits to maintain and use the data in de-identified form and to not attempt to re-identify the data; and (C) contractually obligates any person to whom the covered entity discloses or transfers the de-identified data to comply with the requirements of this paragraph.

(26) DEPLOYER.—The term 'deployer' means any person that uses a high-risk artificial intelligence system, excluding any person who uses such system solely for personal, non-commercial purposes.

(27) DEVELOPER.—The term 'developer' means any person that designs, codes, produces, or substantially modifies an artificial intelligence system, including the architecture, training data, training methodology, or inference mechanisms of such system.

(28) DIGITAL IDENTITY.—The term 'digital identity' means an electronic representation of an individual used for authentication, authorization, or identification purposes, including but not limited to usernames, passwords, biometric templates, cryptographic keys, and digital certificates.

(29) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

(30) DUAL-USE TECHNOLOGY.—The term 'dual-use technology' means technology that has both civilian and military applications and that may pose risks to national security if exported without appropriate controls.

(31) EDGE COMPUTING.—The term 'edge computing' means a distributed computing paradigm that brings computation and data storage closer to the sources of data, rather than relying on a central data center.

(32) EMERGING TECHNOLOGY.—The term 'emerging technology' means technology that is in an early stage of development or adoption but has the potential to significantly affect economic security, national security, or public health and safety, including but not limited to artificial intelligence, quantum computing, biotechnology, advanced materials, autonomous systems, and advanced energy technologies.

(33) ENTITY.—The term 'entity' means any person, partnership, corporation, limited liability company, association, trust, joint venture, or other legal entity, including any governmental entity.

(34) FACIAL RECOGNITION.—The term 'facial recognition' means an automated or semi-automated process that uses biometric data derived from an individual's face to identify or attempt to identify an individual, verify an individual's identity, or assess the characteristics, emotions, or expressions of an individual.

(35) FEDERAL AGENCY.—The term 'Federal agency' has the meaning given the term 'agency' in section 3502 of title 44, United States Code.

(36) FOUNDATION MODEL.—The term 'foundation model' means an AI model that is trained on broad data, generally using self-supervision at scale, and can be adapted to a wide range of downstream tasks. Foundation models include, but are not limited to, large language models, multimodal models, and other general-purpose AI systems.

(37) FRONTIER AI MODEL.—The term 'frontier AI model' means an AI model that: (A) was trained using a quantity of computing power greater than 10 to the power of 26 floating-point operations; (B) demonstrates capabilities that substantially exceed those of prior models; or (C) poses potential risks that the Administrator determines warrant classification as a frontier model.

(38) GENERATIVE AI.—The term 'generative AI' means a category of artificial intelligence techniques that generate novel content, including but not limited to text, images, audio, video, code, or synthetic data, based on patterns learned from training data.

(39) GEOSPATIAL DATA.—The term 'geospatial data' means information that identifies the geographic location of an individual or device, including GPS coordinates, cell tower triangulation data, Wi-Fi positioning data, IP address geolocation, and any other data that can be used to determine location.

(40) GREEN TECHNOLOGY.—The term 'green technology' means any technology, product, or process that: (A) reduces emissions of greenhouse gases or other pollutants; (B) improves energy efficiency; (C) conserves natural resources; (D) reduces waste or promotes recycling and reuse; (E) protects or restores ecosystems; or (F) otherwise contributes to environmental sustainability.

(41) HIGH-RISK AI SYSTEM.—The term 'high-risk AI system' means an AI system that: (A) is used as a safety component of a product, or is itself a product, that is subject to Federal health and safety regulations; (B) is used for biometric identification or categorization of natural persons; (C) is used for the management and operation of critical infrastructure; (D) is used in education or vocational training to determine access, evaluate performance, or monitor individuals; (E) is used in employment contexts for recruiting, screening, hiring, promoting, terminating, or allocating tasks; (F) is used to determine access to essential services or benefits; (G) is used in law enforcement contexts; (H) is used in immigration, asylum, or border control; (I) is used in the administration of justice; or (J) meets other criteria established by the Administrator through rulemaking.

(42) INDIAN TRIBE.—The term 'Indian Tribe' has the meaning given the term 'Indian tribe' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(43) INFORMATION SYSTEM.—The term 'information system' has the meaning given that term in section 3502 of title 44, United States Code.

(44) INTEROPERABILITY.—The term 'interoperability' means the ability of different information technology systems, devices, applications, or products to connect, exchange data, and use data according to a common method that provides consistent, meaningful results.

(45) INTERNET OF THINGS DEVICE.—The term 'Internet of Things device' or 'IoT device' means any device that connects directly or indirectly to the internet and that is capable of collecting, sending, or

receiving data.

(46) LARGE COVERED ENTITY.—The term 'large covered entity' means a covered entity that: (A) had gross revenues in excess of $250,000,000 during the most recent fiscal year; (B) processes the personal data of more than 5,000,000 individuals during any 12-month period; or (C) derives 50 percent or more of its annual revenue from the sale of personal data.

(47) LIMITED-RISK AI SYSTEM.—The term 'limited-risk AI system' means an AI system that: (A) interacts with natural persons; (B) generates or manipulates image, audio, or video content; (C) makes recommendations to individuals; or (D) is used for purposes that do not meet the criteria for high-risk AI systems but that may affect individuals' interests.

(48) MACHINE LEARNING.—The term 'machine learning' means a set of techniques that can be used to train AI models to make predictions or decisions based on data without being explicitly programmed.

(49) MALICIOUS CYBER ACTIVITY.—The term 'malicious cyber activity' means activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.

(50) MINOR.—The term 'minor' means an individual who has not attained the age of 18 years.

(51) NATIONAL TECHNOLOGY GOVERNANCE ADMINISTRATION.—The term 'National Technology Governance Administration' means the agency established under section 901 of this Act.

(52) NATURAL LANGUAGE PROCESSING.—The term 'natural language processing' or 'NLP' means a branch of artificial intelligence that enables computers to understand, interpret, and generate human language.

(53) ONLINE PLATFORM.—The term 'online platform' means any public-facing website, online service, online application, or mobile application that allows users to create an account or profile and that: (A) enables users to create, share, or consume content; (B) facilitates interaction between users; or (C) uses algorithmic processes to determine the content displayed to users.

(54) OPEN-SOURCE SOFTWARE.—The term 'open-source software' means software that is made available under a license that permits users to use, study, modify, and distribute the software and its source code to anyone and for any purpose.

(55) OPERATOR.—The term 'operator' means any person that operates, maintains, or controls a website, online service, online application, or mobile application.

(56) PERSONAL DATA.—The term 'personal data' means any information that identifies or is linked or reasonably linkable to an individual or a device that identifies or is linked or reasonably linkable to an individual, including derived data and unique identifiers.

(57) PREDICTIVE ANALYTICS.—The term 'predictive analytics' means the use of data, statistical algorithms, and machine learning techniques to identify the likelihood of future outcomes based on historical data.

(58) PROCESSING.—The term 'processing' means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, including the collection, creation, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transmission, dissemination, alignment, combination, restriction, erasure, or destruction of personal data.

(59) PROCESSOR.—The term 'processor' means an entity that processes personal data on behalf of a controller.

(60) PROFILING.—The term 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or

movements.

(61) PUBLIC BENEFIT CORPORATION.—The term 'public benefit corporation' means a corporation that is organized under the laws of a State that permits the formation of public benefit corporations and that: (A) identifies in its certificate of incorporation one or more specific public benefits to be promoted by the corporation; and (B) operates in a responsible and sustainable manner.

(62) QUANTUM COMPUTING.—The term 'quantum computing' means computing that harnesses quantum mechanical phenomena, such as superposition, entanglement, and interference, to perform calculations that would be impractical for classical computers.

(63) REASONABLE SECURITY MEASURES.—The term 'reasonable security measures' means administrative, technical, and physical safeguards that are appropriate to: (A) the nature and scope of the activities of the covered entity; (B) the sensitivity of the personal data at issue; (C) the volume and complexity of the personal data at issue; (D) the cost of available tools to improve security; and (E) the current state of the art in administrative, technical, and physical safeguards.

(64) SECRETARY.—Unless otherwise specified, the term 'Secretary' means the Secretary of Commerce.

(65) SENSITIVE COVERED DATA.—The term 'sensitive covered data' means the following forms of personal data: (A) government-issued identification numbers; (B) financial account information; (C) biometric data; (D) genetic data; (E) health data; (F) geolocation data; (G) private communications; (H) account log-in credentials; (I) data revealing racial or ethnic origin, religious beliefs, union membership, sexual orientation, or citizenship or immigration status; (J) data relating to an individual's sexual behavior; (K) calendar data, address book data, phone or text logs, photos, audio recordings, or videos maintained for private use; (L) data collected from a known child; or (M) any other data determined by the Administrator through rulemaking.

(66) SERVICE PROVIDER.—The term 'service provider' means a person that processes personal data on behalf of and at the direction of a covered entity pursuant to a written contract.

(67) SMALL BUSINESS.—The term 'small business' means a covered entity that: (A) has average annual gross revenues of less than $25,000,000 during the preceding three fiscal years; (B) collects or processes the personal data of fewer than 100,000 individuals during any 12-month period; and (C) does not derive 50 percent or more of its annual revenues from the sale of personal data.

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

(69) SYNTHETIC DATA.—The term 'synthetic data' means data that is artificially generated rather than produced by real-world events or processes, including data generated by AI systems.

(70) TARGETED ADVERTISING.—The term 'targeted advertising' means displaying advertisements to an individual based on personal data obtained from that individual's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service on which the advertisement is being displayed.

(71) THIRD PARTY.—The term 'third party' means any person that is not: (A) the covered entity that collected the personal data from the individual; (B) a service provider of such covered entity; or (C) the individual to whom the personal data pertains.

(72) TRAINING DATA.—The term 'training data' means data used to train, validate, or test an AI model, including data used to fine-tune or adapt a pre-trained model.

(73) TRANSPARENCY REPORT.—The term 'transparency report' means a publicly available report that discloses information about a covered entity's data practices, algorithmic systems, content moderation activities, or other activities as required under this Act.

(74) UNDERSERVED COMMUNITY.—The term 'underserved community' means a community with limited access to technology, including communities in rural areas, low-income communities, communities with limited broadband access, communities with limited digital literacy, and communities that have historically been marginalized or disadvantaged.

(75) UNITED STATES PERSON.—The term 'United States person' means: (A) a United States citizen; (B) a lawful permanent resident of the United States; (C) an entity organized under the laws of the United States, any State, or any other jurisdiction within the United States; or (D) any person located in the United States.

CHAPTER 3 - SCOPE AND APPLICATION

SEC. 120. SCOPE OF APPLICATION.

(a) IN GENERAL.—Except as provided in subsection (b), this Act applies to:

(1) all covered entities that process personal data of individuals located in the United States, regardless of where such covered entity is located;

(2) all deployers and developers of artificial intelligence systems that are used within the United States or that process data concerning individuals located in the United States;

(3) all critical infrastructure operators, as defined in section 110;

(4) all Federal agencies, except as otherwise specified in this Act;

(5) all recipients of Federal grants or contracts related to technology development, deployment, or research.

(b) EXCEPTIONS.—This Act does not apply to:

(1) activities of the Federal Government when engaged in national security, intelligence, or law enforcement activities, except as specifically provided in Title IV;

(2) personal data processed by an individual for a purely personal or household activity;

(3) data that has been de-identified in accordance with the requirements of this Act;

(4) publicly available information, except that such exception shall not apply to: (A) biometric data; (B) data collected through scraping or automated means in violation of terms of service; or (C) aggregated data that has been re-identified.

(c) RELATIONSHIP TO OTHER LAWS.—

(1) FEDERAL LAWS.—Nothing in this Act shall be construed to limit, modify, or supersede the requirements of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.), the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), or any other Federal law providing greater protection to individuals.

(2) STATE LAWS.—Except as provided in paragraph (3), this Act shall preempt any State law that relates to the subject matter of this Act.

(3) SAVINGS CLAUSE.—This Act shall not preempt: (A) State consumer protection laws of general applicability; (B) State civil rights laws; (C) State laws governing breach notification, to the extent such laws impose requirements greater than those imposed by this Act; (D) State laws governing student data privacy; or (E) State laws governing employee data privacy.

SEC. 121. EXTRATERRITORIAL APPLICATION.

(a) IN GENERAL.—This Act applies to any covered entity, regardless of where such entity is established, if the entity:

(1) offers products or services to individuals located in the United States;

(2) monitors the behavior of individuals located in the United States; or

(3) processes personal data of individuals located in the United States.

(b) REPRESENTATIVE REQUIREMENT.—Any covered entity subject to this Act that is not established in the United States shall designate a representative in the United States to serve as a point of contact for purposes of compliance and enforcement under this Act.

TITLE II - INFRASTRUCTURE MODERNIZATION

CHAPTER 1 - CRITICAL INFRASTRUCTURE ASSESSMENT

SEC. 201. NATIONAL INFRASTRUCTURE ASSESSMENT.

(a) ASSESSMENT REQUIRED.—Not later than 180 days after the date of enactment of this Act, and every 2 years thereafter, the Secretary, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the heads of other relevant Federal agencies, shall conduct a comprehensive assessment of the Nation's critical infrastructure.

(b) ELEMENTS OF ASSESSMENT.—The assessment required under subsection (a) shall include:

(1) an evaluation of the current state of critical infrastructure across all sectors identified in section 110;

(2) an identification of vulnerabilities in critical infrastructure systems, including both physical and cyber vulnerabilities;

(3) an assessment of the resilience of critical infrastructure to natural disasters, cyberattacks, physical attacks, and other disruptions;

(4) an evaluation of interdependencies between different critical infrastructure sectors;

(5) an identification of infrastructure requiring immediate attention or remediation;

(6) an assessment of workforce needs for infrastructure maintenance and modernization;

(7) an evaluation of the adequacy of existing standards and best practices;

(8) recommendations for infrastructure investments and modernization priorities;

(9) an assessment of emerging technologies that could enhance infrastructure resilience and efficiency;

(10) an evaluation of climate change impacts on critical infrastructure.

(c) CONSULTATION.—In conducting the assessment required under subsection (a), the Secretary shall consult with:

(1) State, local, Tribal, and territorial governments;

(2) owners and operators of critical infrastructure;

(3) relevant industry associations and standards-setting organizations;

(4) academic institutions and research organizations;

(5) labor organizations representing infrastructure workers;

(6) civil society organizations representing affected communities.

(d) REPORT TO CONGRESS.—Not later than 60 days after completing each assessment under subsection (a), the Secretary shall submit to the appropriate congressional committees a report containing the findings and recommendations of such assessment. Such report shall be submitted in both classified and unclassified forms as appropriate.

SEC. 202. INFRASTRUCTURE MODERNIZATION PRIORITIES.

(a) ESTABLISHMENT OF PRIORITIES.—Based on the assessment conducted under section 201, the Secretary shall establish national priorities for infrastructure modernization.

(b) CRITERIA.—In establishing priorities under subsection (a), the Secretary shall consider:

(1) the severity of identified vulnerabilities and risks;

(2) the potential consequences of infrastructure failure or disruption;

(3) the number of individuals and communities affected;

(4) the availability of cost-effective remediation measures;

(5) the potential for leveraging private sector investment;

(6) environmental and sustainability considerations;

(7) equity considerations, including impacts on underserved communities;

(8) alignment with national security objectives.

CHAPTER 2 - BROADBAND AND TELECOMMUNICATIONS

SEC. 210. UNIVERSAL BROADBAND ACCESS.

(a) FINDINGS.—Congress finds the following:

(1) Access to high-speed broadband internet is essential for full participation in modern economic, educational, and civic life.

(2) Approximately 21 million Americans lack access to broadband internet that meets minimum speed standards, with disproportionate impacts on rural communities, low-income households, and communities of color.

(3) The digital divide threatens to exacerbate existing social and economic inequalities and limit opportunities for millions of Americans.

(4) Federal investment in broadband infrastructure can catalyze private sector investment and accelerate deployment in underserved areas.

(5) The COVID-19 pandemic demonstrated the critical importance of reliable broadband access for remote work, telehealth, distance learning, and maintaining social connections.

(b) UNIVERSAL SERVICE GOAL.—It is the goal of the United States that every household and business in the Nation shall have access to reliable, affordable, high-speed broadband internet service by December 31, 2030.

(c) MINIMUM STANDARDS.—For purposes of this section, 'high-speed broadband internet service' means broadband internet access service with:

(1) download speeds of at least 100 megabits per second;

(2) upload speeds of at least 20 megabits per second; and

(3) latency sufficient to support real-time interactive applications.

(d) REVIEW OF STANDARDS.—Not later than 2 years after the date of enactment of this Act, and every 2 years thereafter, the Federal Communications Commission shall review and, as appropriate, update the minimum standards under subsection (c) to reflect technological advancements and evolving user needs.

SEC. 211. BROADBAND INFRASTRUCTURE PROGRAM.

(a) ESTABLISHMENT.—There is established within the National Telecommunications and Information Administration a program, to be known as the 'National Broadband Infrastructure Program', to provide grants, loans, and other financial assistance to eligible entities for the deployment and improvement of broadband infrastructure in unserved and underserved areas.

(b) ELIGIBLE ENTITIES.—The following entities are eligible to receive assistance under this section:

(1) State, local, Tribal, and territorial governments;

(2) political subdivisions of States;

(3) cooperatives, including electric cooperatives and telephone cooperatives;

(4) nonprofit organizations;

(5) public-private partnerships;

(6) telecommunications providers;

(7) electric utilities.

(c) ELIGIBLE USES.—Assistance provided under this section may be used for:

(1) construction of new broadband infrastructure, including fiber optic networks, fixed wireless systems, and satellite-based systems;

(2) upgrade of existing broadband infrastructure to meet minimum speed standards;

(3) acquisition of rights-of-way, easements, and other property interests necessary for broadband deployment;

(4) engineering, design, and planning activities;

(5) workforce development and training for broadband deployment and maintenance;

(6) community anchor institution connections, including connections to schools, libraries, healthcare facilities, and government buildings;

(7) middle-mile infrastructure to connect local networks to internet exchange points.

(d) PRIORITIZATION.—In awarding assistance under this section, the Assistant Secretary shall prioritize projects that:

(1) serve unserved areas, defined as areas where at least 90 percent of households lack access to broadband service meeting minimum speed standards;

(2) serve high-cost areas where private sector deployment is economically challenging;

(3) deploy fiber optic technology or other technology providing scalable capacity;

(4) demonstrate strong community support and participation;

(5) incorporate sustainable and resilient design principles;

(6) create good-paying jobs with benefits, including through the use of project labor agreements;

(7) promote competition in the broadband market.

SEC. 212. DIGITAL EQUITY INITIATIVES.

(a) DIGITAL EQUITY GRANTS.—The Assistant Secretary shall establish a grant program to support digital equity initiatives that promote:

(1) digital literacy training for individuals of all ages;

(2) affordability programs to reduce the cost of broadband service and devices for low-income households;

(3) accessibility improvements for individuals with disabilities;

(4) multilingual digital resources and support;

(5) public computer access and technical assistance;

(6) cybersecurity education and awareness;

(7) telehealth readiness and adoption.

(b) AFFORDABLE CONNECTIVITY PROGRAM.—

(1) ESTABLISHMENT.—There is established an Affordable Connectivity Program to provide subsidies to eligible households for broadband internet service and connected devices.

(2) ELIGIBILITY.—A household is eligible for the Affordable Connectivity Program if the household income is at or below 200 percent of the Federal Poverty Guidelines, or if a member of the household participates in a Federal, State, or Tribal assistance program, including: (A) the Supplemental Nutrition Assistance Program; (B) Medicaid; (C) the Special Supplemental Nutrition Program for Women, Infants, and Children; (D) Supplemental Security Income; (E) Federal Public Housing Assistance; (F) the Veterans Pension and Survivors Benefit; or (G) the Free and Reduced Price School Lunch Program.

(3) BENEFIT AMOUNT.—An eligible household may receive a monthly subsidy of up to $30 for broadband service, or up to $75 for households on qualifying Tribal lands, and a one-time subsidy of up to $100 for a laptop, desktop computer, or tablet.

CHAPTER 3 - TRANSPORTATION INFRASTRUCTURE

SEC. 220. TRANSPORTATION TECHNOLOGY MODERNIZATION.

(a) IN GENERAL.—The Secretary of Transportation shall develop and implement a comprehensive strategy for modernizing the Nation's transportation infrastructure through the deployment of advanced technologies.

(b) ELEMENTS.—The strategy required under subsection (a) shall address:

(1) integration of intelligent transportation systems across all modes of transportation;

(2) deployment of vehicle-to-infrastructure and vehicle-to-vehicle communication systems;

(3) preparation of roadways and other infrastructure for autonomous and connected vehicles;

(4) modernization of traffic management systems using artificial intelligence and real-time data analytics;

(5) electrification of transportation systems, including deployment of electric vehicle charging infrastructure;

(6) integration of shared mobility services with public transit systems;

(7) cybersecurity for connected transportation systems;

(8) accessibility improvements for individuals with disabilities;

(9) resilience to climate change impacts and extreme weather events.

SEC. 221. AUTONOMOUS VEHICLE FRAMEWORK.

(a) REGULATORY FRAMEWORK.—Not later than 2 years after the date of enactment of this Act, the Secretary of Transportation shall, in consultation with the Administrator of the National Highway Traffic Safety Administration and other relevant agencies, establish a comprehensive regulatory framework for the testing and deployment of autonomous vehicles on public roadways.

(b) FRAMEWORK REQUIREMENTS.—The framework established under subsection (a) shall include:

(1) safety standards for autonomous vehicles at each level of automation, as defined by SAE International;

(2) requirements for testing and validation of autonomous vehicle systems, including simulation testing, closed-course testing, and on-road testing;

(3) cybersecurity requirements for autonomous vehicle systems, including protection against remote attacks and unauthorized access;

(4) data collection and reporting requirements, including requirements for reporting accidents, near-misses, and system disengagements;

(5) requirements for human-machine interfaces and driver monitoring systems in vehicles with conditional automation;

(6) privacy protections for data collected by autonomous vehicles, consistent with the requirements of Title V of this Act;

(7) accessibility requirements for autonomous vehicles serving individuals with disabilities;

(8) requirements for interaction between autonomous vehicles and vulnerable road users, including pedestrians, cyclists, and motorcyclists;

(9) minimum insurance and liability requirements;

(10) procedures for recall and remediation of safety defects.

(c) STATE PREEMPTION.—

(1) PERFORMANCE STANDARDS.—State laws relating to the performance standards for autonomous vehicles and autonomous vehicle systems are preempted to the extent that they conflict with the requirements established under this section.

(2) SAVINGS CLAUSE.—Nothing in this section shall be construed to preempt State laws relating to: (A) registration, licensing, and titling of vehicles; (B) insurance requirements; (C) traffic laws and enforcement; (D) liability for accidents; or (E) other matters traditionally regulated by States.

CHAPTER 4 - ENERGY INFRASTRUCTURE

SEC. 230. GRID MODERNIZATION.

(a) IN GENERAL.—The Secretary of Energy shall establish a program to accelerate the modernization of the Nation's electric grid to enhance reliability, resilience, security, and efficiency.

(b) PROGRAM ELEMENTS.—The program established under subsection (a) shall support:

(1) deployment of advanced metering infrastructure and smart grid technologies;

(2) integration of distributed energy resources, including rooftop solar, battery storage, and electric vehicles;

(3) deployment of grid-scale energy storage systems;

(4) upgrade of transmission infrastructure to reduce congestion and enable delivery of renewable energy;

(5) deployment of advanced sensors and monitoring systems for real-time grid visibility;

(6) implementation of advanced analytics and artificial intelligence for grid optimization;

(7) hardening of grid infrastructure against extreme weather events and physical attacks;

(8) cybersecurity improvements for grid control systems;

(9) interoperability standards for grid-connected devices;

(10) workforce training for grid modernization technologies.

SEC. 231. GRID CYBERSECURITY.

(a) MANDATORY CYBERSECURITY STANDARDS.—Not later than 18 months after the date of enactment of this Act, the Secretary of Energy, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency and the Federal Energy Regulatory Commission, shall establish mandatory cybersecurity standards for the bulk electric system.

(b) STANDARD REQUIREMENTS.—The standards established under subsection (a) shall address:

(1) access control and identity management;

(2) network segmentation and monitoring;

(3) vulnerability management and patching;

(4) incident detection and response;

(5) supply chain security;

(6) physical security of cyber assets;

(7) training and awareness programs;

(8) third-party risk management;

(9) recovery and restoration procedures.

CHAPTER 5 - WATER INFRASTRUCTURE

SEC. 240. WATER SYSTEM MODERNIZATION.

(a) IN GENERAL.—The Administrator of the Environmental Protection Agency shall establish a program to support the modernization of water and wastewater infrastructure across the United States.

(b) ELIGIBLE PROJECTS.—Projects eligible for support under this section include:

(1) replacement of aging water mains, service lines, and other distribution infrastructure;

(2) replacement of lead service lines and remediation of lead contamination;

(3) installation of advanced water treatment technologies;

(4) deployment of smart water management systems, including leak detection and pressure management;

(5) water recycling and reuse systems;

(6) stormwater management and green infrastructure;

(7) wastewater treatment upgrades, including nutrient removal;

(8) combined sewer overflow remediation;

(9) dam safety improvements;

(10) drought resilience and water conservation measures.

TITLE III - ARTIFICIAL INTELLIGENCE GOVERNANCE

CHAPTER 1 - AI RISK CLASSIFICATION FRAMEWORK

SEC. 301. AI RISK CLASSIFICATION.

(a) ESTABLISHMENT OF CLASSIFICATION FRAMEWORK.—The Administrator shall establish a risk-based classification framework for artificial intelligence systems that categorizes AI systems based on the level of risk they pose to individuals, communities, and society.

(b) RISK CATEGORIES.—The framework established under subsection (a) shall include the following categories:

(1) UNACCEPTABLE RISK.—AI systems that pose an unacceptable risk to safety, fundamental rights, or democratic values shall be prohibited. Such systems include, but are not limited to:

(A) AI systems that deploy subliminal techniques beyond a person's consciousness to materially distort behavior in a manner likely to cause physical or psychological harm;

(B) AI systems that exploit vulnerabilities of specific groups, such as children, individuals with disabilities, or individuals in economic distress, to materially distort behavior in a harmful manner;

(C) AI systems that evaluate or classify individuals based on social behavior or personal characteristics in ways that lead to detrimental treatment unrelated to the original context in which data was collected;

(D) AI systems that enable real-time biometric identification in publicly accessible spaces for law enforcement purposes, except in narrowly defined circumstances with judicial authorization;

(E) AI systems that predict the likelihood of an individual committing criminal offenses based solely on profiling or personality traits;

(F) AI systems designed to generate synthetic media of real individuals without consent for purposes of harassment, fraud, or defamation.

(2) HIGH-RISK.—High-risk AI systems, as defined in section 110, shall be subject to the requirements set forth in Chapter 2 of this Title.

(3) LIMITED-RISK.—Limited-risk AI systems shall be subject to transparency requirements set forth in Chapter 3 of this Title.

(4) MINIMAL-RISK.—AI systems that pose minimal risk to individuals or society are not subject to the specific requirements of this Title, although developers and deployers of such systems are encouraged to adopt voluntary codes of conduct.

(c) CLASSIFICATION CRITERIA.—In classifying AI systems under this section, the Administrator shall consider:

(1) the intended purpose and use context of the AI system;

(2) the nature and extent of human oversight in the system's operation;

(3) the reversibility of decisions made or supported by the system;

(4) the availability of alternative means for affected individuals;

(5) the scale of potential impact, including the number of affected individuals;

(6) the vulnerability of affected populations;

(7) the potential for disparate impact on protected groups;

(8) the severity of potential harms, including physical, psychological, financial, and reputational harms;

(9) the level of autonomy of the system;

(10) the opacity or explainability of the system.

SEC. 302. CLASSIFICATION PROCEDURES.

(a) SELF-CLASSIFICATION.—Developers of AI systems shall conduct an initial classification of their systems under the framework established in section 301 prior to placing such systems on the market or putting them into service.

(b) DOCUMENTATION.—Developers shall document their classification determination, including:

(1) the intended purpose and use context of the system;

(2) the factors considered in making the classification determination;

(3) the rationale for the classification assigned;

(4) any assumptions or limitations of the analysis.

(c) ADMINISTRATOR REVIEW.—The Administrator may review classification determinations and require reclassification if the Administrator determines that: (1) the classification was made in error; (2) new information about the system's capabilities or impacts warrants reclassification; or (3) the system is being used in ways not contemplated in the original classification.

CHAPTER 2 - HIGH-RISK AI SYSTEMS

SEC. 310. REQUIREMENTS FOR HIGH-RISK AI SYSTEMS.

(a) IN GENERAL.—Prior to placing a high-risk AI system on the market or putting it into service, the developer shall ensure that the system meets the requirements set forth in this section.

(b) RISK MANAGEMENT SYSTEM.—Developers of high-risk AI systems shall establish, implement, document, and maintain a risk management system that:

(1) identifies and analyzes known and reasonably foreseeable risks that the system may pose to health, safety, and fundamental rights;

(2) estimates and evaluates risks arising from the intended use of the system and reasonably foreseeable misuse;

(3) evaluates risks based on data gathered from post-market monitoring systems;

(4) adopts suitable risk management measures to address identified risks;

(5) includes testing procedures to ensure risks remain at acceptable levels throughout the system lifecycle.

(c) DATA GOVERNANCE.—Developers of high-risk AI systems shall implement data governance and management practices that ensure:

(1) training, validation, and testing datasets are relevant, representative, and, to the best extent possible, free from errors and bias;

(2) appropriate data quality criteria are established for the specific use case;

(3) examination of potential biases that may affect the health, safety, or fundamental rights of individuals or lead to discrimination;

(4) appropriate measures to address identified biases are implemented;

(5) personal data used in training is processed in compliance with applicable privacy requirements, including those set forth in Title V of this Act.

(d) TECHNICAL DOCUMENTATION.—Developers shall prepare technical documentation that contains, at a minimum:

(1) a general description of the AI system, including its intended purpose, the persons and systems involved in its development, and the date and version of the system;

(2) a detailed description of the elements of the AI system and the process for its development, including training methodologies and techniques, design specifications, and key design choices;

(3) a description of the data used for training, validation, and testing, including the characteristics and sources of such data, data collection procedures, data preparation and labeling methods, and relevant data limitations;

(4) information on the system's performance, including performance metrics, limitations, and known or foreseeable circumstances that may affect performance;

(5) a description of the risk management system implemented pursuant to subsection (b);

(6) a description of relevant changes to the system through its lifecycle;

(7) instructions for use, including information on how to interpret system outputs.

(e) RECORD-KEEPING.—High-risk AI systems shall be designed and developed with logging capabilities that enable:

(1) recording of events relevant to identifying risks and substantial modifications throughout the system lifecycle;

(2) identification of periods during which the system was in use;

(3) preservation of logs for a period appropriate to the intended purpose and applicable legal obligations;

(4) protection of logs against unauthorized modification or deletion.

(f) TRANSPARENCY.—High-risk AI systems shall be designed and developed to ensure that:

(1) their operation is sufficiently transparent to enable deployers to interpret system outputs and use them appropriately;

(2) affected individuals can be informed when they are subject to a decision made or supported by the system;

(3) affected individuals can obtain meaningful explanation of decisions affecting them;

(4) deployers understand the capabilities and limitations of the system.

(g) HUMAN OVERSIGHT.—High-risk AI systems shall be designed and developed to enable appropriate human oversight, including:

(1) measures enabling individuals overseeing the system to fully understand its capabilities and limitations;

(2) measures enabling individuals to correctly interpret system outputs;

(3) ability for individuals to decide, in specific situations, not to use the system or to disregard, override, or reverse system outputs;

(4) ability to intervene on the operation of the system or to interrupt the system through a 'stop' function.

(h) ACCURACY, ROBUSTNESS, AND CYBERSECURITY.—High-risk AI systems shall be designed and developed so that they achieve:

(1) an appropriate level of accuracy, robustness, and cybersecurity, and perform consistently throughout their lifecycle;

(2) resilience against attempts by unauthorized third parties to alter their use or performance;

(3) protection against vulnerabilities that could permit unauthorized access;

(4) accuracy levels appropriate for their intended purpose, with declared accuracy metrics.

SEC. 311. CONFORMITY ASSESSMENT.

(a) CONFORMITY ASSESSMENT REQUIRED.—Prior to placing a high-risk AI system on the market or putting it into service, the developer shall conduct a conformity assessment to demonstrate compliance with the requirements set forth in section 310.

(b) ASSESSMENT PROCEDURES.—The Administrator shall, by regulation, establish procedures for conformity assessments that are proportionate to the level of risk posed by the AI system and the context of its deployment.

(c) THIRD-PARTY ASSESSMENT.—For certain categories of high-risk AI systems to be determined by the Administrator, conformity assessment shall be conducted by an accredited third-party assessment body.

(d) CONFORMITY DECLARATION.—Upon successful completion of the conformity assessment, the developer shall draw up a written declaration of conformity and affix a compliance marking to the system.

SEC. 312. DEPLOYER OBLIGATIONS.

(a) IN GENERAL.—Deployers of high-risk AI systems shall:

(1) use the system in accordance with the instructions of use accompanying the system;

(2) ensure that input data is relevant and sufficiently representative in view of the intended purpose;

(3) monitor the operation of the system and inform the developer of serious incidents or malfunctions;

(4) keep logs automatically generated by the system, to the extent under their control;

(5) conduct an impact assessment prior to deploying the system, as required under Chapter 4 of this Title;

(6) ensure that individuals subject to decisions made or supported by the system are informed of such use and can obtain meaningful explanation of decisions affecting them;

(7) ensure that human oversight is exercised as required under section 310(g).

(b) IMPACT ASSESSMENTS.—Before deploying a high-risk AI system, deployers shall conduct an algorithmic impact assessment in accordance with the requirements of Chapter 4 of this Title.

CHAPTER 3 - AI TRANSPARENCY AND ACCOUNTABILITY

SEC. 320. TRANSPARENCY REQUIREMENTS FOR AI SYSTEMS.

(a) DISCLOSURE OF AI USE.—Any person that deploys an AI system to interact with individuals shall disclose to such individuals, in a clear and conspicuous manner, that they are interacting with an AI system.

(b) DISCLOSURE OF SYNTHETIC CONTENT.—Any person that generates or distributes synthetic audio, image, or video content shall:

(1) clearly label such content as AI-generated or manipulated in a manner that is detectable by individuals and, where technically feasible, by automated detection systems;

(2) include provenance information indicating the origin and modification history of the content;

(3) not remove, disable, or otherwise circumvent labeling or provenance information.

(c) EXCEPTIONS.—The requirements of subsection (b) shall not apply to:

(1) synthetic content that is obviously artistic, satirical, or fictional;

(2) content generated for legitimate research purposes;

(3) content that does not depict real individuals or could not reasonably be mistaken for authentic content.

SEC. 321. ACCOUNTABILITY FOR AI SYSTEMS.

(a) DESIGNATION OF RESPONSIBLE PERSON.—Each developer and deployer of a high-risk AI system shall designate at least one individual to be responsible for ensuring compliance with the requirements of this Title.

(b) INCIDENT REPORTING.—

(1) SERIOUS INCIDENTS.—Developers and deployers of high-risk AI systems shall report to the Administrator any serious incident or malfunctioning of such systems that constitutes a breach of obligations under Federal or State law intended to protect fundamental rights or causes harm to individuals or groups.

(2) TIMELINE.—Reports under paragraph (1) shall be submitted: (A) within 72 hours of the developer or deployer becoming aware of the incident for incidents involving risk to life or safety; or (B) within 30 days for other serious incidents.

(c) AUDIT REQUIREMENTS.—Large covered entities that deploy high-risk AI systems shall conduct annual audits of such systems to assess compliance with the requirements of this Title and shall make the results of such audits available to the Administrator upon request.

CHAPTER 4 - ALGORITHMIC IMPACT ASSESSMENTS

SEC. 330. ALGORITHMIC IMPACT ASSESSMENT REQUIREMENTS.

(a) ASSESSMENT REQUIRED.—Any covered entity that uses a covered algorithm to make or materially support a consequential decision shall conduct and document an algorithmic impact assessment prior to deploying such algorithm and periodically thereafter.

(b) ASSESSMENT CONTENTS.—An algorithmic impact assessment shall include:

(1) a description of the covered algorithm, including its purpose, intended uses, and technical specifications;

(2) an assessment of the necessity and proportionality of using the covered algorithm for the stated purpose;

(3) an evaluation of potential adverse impacts on the rights, safety, and well-being of affected individuals, including potential impacts on protected classes under Federal civil rights laws;

(4) an assessment of the data used to train and operate the algorithm, including an evaluation of data quality, representativeness, and potential biases;

(5) an evaluation of the algorithm's accuracy, including performance across different demographic groups;

(6) a description of safeguards implemented to address identified risks, including human oversight mechanisms;

(7) an assessment of the transparency and explainability of the algorithm;

(8) a description of the process for individuals to contest or appeal decisions made using the algorithm;

(9) a plan for ongoing monitoring and evaluation of the algorithm's performance.

(c) TIMING.—Algorithmic impact assessments shall be conducted:

(1) prior to initial deployment of the covered algorithm;

(2) prior to any substantial modification to the algorithm or its use context;

(3) at least annually for algorithms in continuous use;

(4) upon request by the Administrator following a credible complaint or report of harm.

SEC. 331. DISPARATE IMPACT EVALUATION.

(a) EVALUATION REQUIRED.—As part of the algorithmic impact assessment required under section 330, covered entities shall evaluate whether the covered algorithm produces disparate impacts on individuals based on race, color, national origin, sex, religion, age, disability, or other characteristics protected under Federal civil rights laws.

(b) METHODOLOGY.—The Administrator shall, by regulation, establish standards and methodologies for conducting disparate impact evaluations that are appropriate for different types of covered algorithms and use contexts.

(c) MITIGATION.—If a disparate impact evaluation reveals that a covered algorithm produces unlawful disparate impacts, the covered entity shall:

(1) take reasonable steps to mitigate the identified disparate impacts;

(2) document the steps taken and their effectiveness;

(3) if disparate impacts cannot be adequately mitigated, discontinue use of the algorithm for the affected use case unless the entity can demonstrate that the algorithm is job-related and consistent with business necessity, and there is no less discriminatory alternative available.

CHAPTER 5 - AI SAFETY STANDARDS

SEC. 340. NATIONAL AI SAFETY STANDARDS.

(a) DEVELOPMENT OF STANDARDS.—The Administrator, in consultation with the Director of the National Institute of Standards and Technology, shall develop voluntary consensus standards for the safe development, testing, and deployment of AI systems.

(b) STANDARD ELEMENTS.—The standards developed under subsection (a) shall address:

(1) testing and evaluation methodologies for AI systems;

(2) benchmarks for measuring AI system performance, including accuracy, fairness, robustness, and security;

(3) red teaming and adversarial testing practices;

(4) safety considerations for foundation models and frontier AI;

(5) documentation and transparency practices;

(6) human oversight requirements;

(7) incident reporting and response;

(8) secure development lifecycle practices;

(9) interpretability and explainability methods;

(10) data quality and governance practices.

SEC. 341. FRONTIER AI SAFETY.

(a) ADDITIONAL REQUIREMENTS FOR FRONTIER AI.—Developers of frontier AI models, as defined in section 110, shall, in addition to the requirements otherwise applicable under this Title:

(1) conduct comprehensive safety evaluations prior to deployment, including evaluations for dangerous capabilities such as the ability to assist in the development of weapons, conduct cyberattacks, or manipulate individuals or systems;

(2) implement robust safety measures and safeguards to prevent misuse;

(3) maintain the capability to monitor and respond to emerging risks throughout the model's deployment;

(4) notify the Administrator prior to deploying frontier AI models;

(5) provide the Administrator with access to model capabilities for safety evaluation purposes upon request;

(6) participate in information sharing regarding safety incidents and emerging risks.

(b) COMPUTING THRESHOLD NOTIFICATION.—Any person conducting a training run that exceeds the computing threshold specified in section 110(42) shall notify the Administrator within 10 days of commencing such training run.

TITLE IV - CYBERSECURITY ENHANCEMENT

CHAPTER 1 - NATIONAL CYBERSECURITY STRATEGY

SEC. 401. NATIONAL CYBERSECURITY STRATEGY.

(a) STRATEGY REQUIRED.—The President shall develop and implement a comprehensive national cybersecurity strategy to protect the Nation's critical infrastructure, government systems, private enterprises, and citizens from cyber threats.

(b) ELEMENTS.—The strategy required under subsection (a) shall include:

(1) an assessment of current and emerging cyber threats to the Nation;

(2) goals and objectives for improving the Nation's cybersecurity posture;

(3) a plan for protecting critical infrastructure across all sectors;

(4) a plan for securing Federal information systems;

(5) a framework for public-private cooperation on cybersecurity;

(6) initiatives to develop and retain a skilled cybersecurity workforce;

(7) a research and development agenda for cybersecurity technologies;

(8) a plan for international cooperation on cybersecurity issues;

(9) metrics for measuring progress toward cybersecurity goals;

(10) provisions for regular review and updating of the strategy.

SEC. 402. COORDINATION OF CYBERSECURITY ACTIVITIES.

(a) NATIONAL CYBER DIRECTOR.—There is established within the Executive Office of the President the position of National Cyber Director, who shall serve as the principal advisor to the President on cybersecurity policy and strategy.

(b) RESPONSIBILITIES.—The National Cyber Director shall:

(1) lead the development and implementation of the national cybersecurity strategy;

(2) coordinate cybersecurity activities across Federal agencies;

(3) advise the President on cybersecurity-related budget priorities;

(4) lead interagency processes for addressing cybersecurity incidents and threats;

(5) engage with the private sector, State and local governments, and international partners on cybersecurity issues;

(6) report to Congress on cybersecurity matters as required.

CHAPTER 2 - CRITICAL INFRASTRUCTURE PROTECTION

SEC. 410. CRITICAL INFRASTRUCTURE CYBERSECURITY REQUIREMENTS.

(a) MINIMUM REQUIREMENTS.—Owners and operators of critical infrastructure shall implement cybersecurity measures that meet or exceed the minimum requirements established by the Director pursuant to this section.

(b) SECTOR-SPECIFIC REQUIREMENTS.—The Director, in coordination with relevant sector risk management agencies, shall establish sector-specific cybersecurity requirements that address the unique risks and characteristics of each critical infrastructure sector.

(c) RISK-BASED APPROACH.—The requirements established under this section shall be risk-based and shall take into account:

(1) the criticality of the infrastructure to national security, economic security, and public health and safety;

(2) the potential consequences of a successful cyberattack;

(3) the current threat landscape and known vulnerabilities;

(4) the size and resources of the infrastructure owner or operator;

(5) the availability and cost of cybersecurity measures.

SEC. 411. SUPPLY CHAIN SECURITY.

(a) SUPPLY CHAIN RISK MANAGEMENT.—Owners and operators of critical infrastructure shall implement supply chain risk management programs that:

(1) identify and assess supply chain risks associated with information and communications technology and services;

(2) establish vendor security requirements and evaluation processes;

(3) monitor suppliers for security incidents and vulnerabilities;

(4) develop contingency plans for supply chain disruptions;

(5) maintain a software bill of materials for critical systems.

(b) PROHIBITED EQUIPMENT.—The Director shall maintain a list of information and communications technology and services that pose unacceptable national security risks and are prohibited from use in critical infrastructure systems.

CHAPTER 3 - INCIDENT RESPONSE AND REPORTING

SEC. 420. CYBERSECURITY INCIDENT REPORTING.

(a) REPORTING REQUIREMENT.—

(1) COVERED INCIDENTS.—A covered entity that experiences a covered cybersecurity incident shall report such incident to the Director in accordance with this section.

(2) COVERED CYBERSECURITY INCIDENT DEFINED.—For purposes of this section, a 'covered cybersecurity incident' means a cybersecurity incident that: (A) results in substantial loss of confidentiality, integrity, or availability of a covered entity's information system or data; (B) results in unauthorized access to sensitive data; (C) has a significant impact on safety systems; (D) disrupts business operations for more than 24 hours; or (E) meets other criteria established by the Director.

(b) TIMELINE.—Reports required under subsection (a) shall be submitted:

(1) within 72 hours of reasonably believing that a covered cybersecurity incident has occurred;

(2) within 24 hours if the incident involves ransomware;

(3) within 24 hours of making any ransom payment related to a cybersecurity incident;

(4) supplemental reports shall be submitted as additional information becomes available.

(c) REPORT CONTENTS.—Reports submitted under this section shall include, to the extent known:

(1) a description of the incident, including the date, time, and duration;

(2) an assessment of the systems, data, and functions affected;

(3) an assessment of the impact on operations;

(4) information about the type of vulnerability exploited;

(5) tactics, techniques, and procedures used by the threat actor, if known;

(6) any indicators of compromise;

(7) remediation activities undertaken or planned;

(8) contact information for incident response.

SEC. 421. INCIDENT RESPONSE CAPABILITIES.

(a) NATIONAL INCIDENT RESPONSE PLAN.—The Director shall develop and maintain a national cyber incident response plan that provides a framework for coordinated response to significant cybersecurity incidents.

(b) INCIDENT RESPONSE ASSISTANCE.—The Director shall provide, upon request, technical assistance to critical infrastructure owners and operators experiencing significant cybersecurity incidents.

CHAPTER 4 - CYBERSECURITY WORKFORCE DEVELOPMENT

SEC. 430. CYBERSECURITY WORKFORCE INITIATIVE.

(a) ESTABLISHMENT.—There is established the National Cybersecurity Workforce Initiative to address the shortage of skilled cybersecurity professionals in the United States.

(b) PROGRAM ELEMENTS.—The Initiative shall include:

(1) scholarships and loan forgiveness programs for students pursuing cybersecurity degrees or certifications in exchange for service in government or critical infrastructure sectors;

(2) grants to educational institutions to develop or expand cybersecurity programs;

(3) support for apprenticeship programs in cybersecurity;

(4) cybersecurity education initiatives for K-12 students;

(5) programs to increase diversity in the cybersecurity workforce;

(6) continuing education and upskilling programs for current cybersecurity professionals;

(7) programs to facilitate the transition of veterans to cybersecurity careers;

(8) public awareness campaigns to promote cybersecurity careers.

TITLE V - DIGITAL RIGHTS AND PRIVACY

CHAPTER 1 - CONSUMER DATA PROTECTION

SEC. 501. CONSUMER DATA RIGHTS.

(a) RIGHT TO ACCESS.—An individual has the right to obtain from a covered entity confirmation as to whether personal data concerning the individual is being processed and, where that is the case, access to the personal data and the following information:

(1) the purposes of the processing;

(2) the categories of personal data concerned;

(3) the recipients or categories of recipients to whom the personal data has been or will be disclosed;

(4) where possible, the envisaged period for which the personal data will be stored, or the criteria used to determine that period;

(5) the existence of the right to request rectification or erasure of personal data;

(6) the right to lodge a complaint with the Commission;

(7) where the personal data is not collected from the individual, any available information as to its source;

(8) the existence of automated decision-making, including profiling, and meaningful information about the logic involved.

(b) RIGHT TO CORRECTION.—An individual has the right to obtain from a covered entity the rectification of inaccurate personal data concerning the individual without undue delay.

(c) RIGHT TO DELETION.—An individual has the right to obtain from a covered entity the erasure of personal data concerning the individual without undue delay where:

(1) the personal data is no longer necessary in relation to the purposes for which it was collected;

(2) the individual withdraws consent on which the processing is based and there is no other legal ground for the processing;

(3) the individual objects to the processing and there are no overriding legitimate grounds for the processing;

(4) the personal data has been unlawfully processed;

(5) the personal data has to be erased for compliance with a legal obligation.

(d) RIGHT TO PORTABILITY.—An individual has the right to receive the personal data concerning the individual which the individual has provided to a covered entity in a structured, commonly used, and machine-readable format and has the right to transmit that data to another entity without hindrance from the covered entity.

(e) RIGHT TO OPT OUT.—An individual has the right to opt out of:

(1) the sale or sharing of personal data;

(2) targeted advertising;

(3) profiling in furtherance of decisions that produce legal or similarly significant effects concerning the individual;

(4) the processing of sensitive covered data for purposes not expressly authorized by the individual.

SEC. 502. COVERED ENTITY OBLIGATIONS.

(a) DATA MINIMIZATION.—A covered entity shall limit the collection of personal data to what is directly relevant and necessary to accomplish a specific purpose disclosed to the individual.

(b) PURPOSE LIMITATION.—A covered entity shall not process personal data in a manner that is incompatible with the purposes for which it was collected, except with the express consent of the individual or as otherwise authorized by law.

(c) RETENTION LIMITATION.—A covered entity shall not retain personal data for longer than is necessary to accomplish the purpose for which it was collected, unless retention is required by law.

(d) SECURITY.—A covered entity shall establish, implement, and maintain reasonable security practices and procedures to protect personal data from unauthorized access, use, disclosure, and destruction.

(e) TRANSPARENCY.—A covered entity shall make publicly available a privacy policy that clearly and conspicuously describes:

(1) the categories of personal data the covered entity collects;

(2) the purposes for which each category of personal data is collected and used;

(3) the categories of personal data that the covered entity sells or shares with third parties;

(4) the categories of third parties to whom the covered entity sells or shares personal data;

(5) the rights of individuals under this Act and how to exercise such rights;

(6) the retention periods for each category of personal data;

(7) contact information for inquiries and complaints.

SEC. 503. CONSENT REQUIREMENTS.

(a) GENERAL CONSENT STANDARD.—Where processing is based on consent, the covered entity shall be able to demonstrate that the individual has consented to processing of his or her personal data.

(b) AFFIRMATIVE EXPRESS CONSENT.—Affirmative express consent shall be required for:

(1) processing of sensitive covered data;

(2) transfer of personal data to third parties for purposes unrelated to the original collection;

(3) use of personal data for targeted advertising;

(4) collection of biometric data;

(5) collection of geolocation data revealing the individual's movements over time.

(c) WITHDRAWAL OF CONSENT.—The individual shall have the right to withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Before giving consent, the individual shall be informed of the right to withdraw. It shall be as easy to withdraw consent as to give it.

CHAPTER 2 - DIGITAL IDENTITY MANAGEMENT

SEC. 510. DIGITAL IDENTITY FRAMEWORK.

(a) ESTABLISHMENT.—The Administrator shall establish a national framework for secure, privacy-preserving digital identity that enables individuals to prove their identity online while minimizing the collection and exposure of personal data.

(b) FRAMEWORK PRINCIPLES.—The framework established under subsection (a) shall be designed to:

(1) minimize the amount of personal data required to be disclosed in identity verification transactions;

(2) enable selective disclosure of attributes without revealing unnecessary personal information;

(3) protect against identity theft and fraud;

(4) preserve individual privacy and autonomy;

(5) support interoperability across public and private sector systems;

(6) be accessible to individuals regardless of technical sophistication or disability;

(7) be voluntary for individuals to adopt and use.

CHAPTER 3 - ALGORITHMIC RIGHTS

SEC. 520. RIGHT TO EXPLANATION.

(a) IN GENERAL.—An individual who is subject to a consequential decision made or materially supported by a covered algorithm has the right to obtain from the covered entity:

(1) notice that a covered algorithm was used in making or materially supporting the decision;

(2) a meaningful explanation of the decision, including the principal factors that led to the decision and how those factors were weighted;

(3) information about the individual's right to contest the decision.

(b) FORM OF EXPLANATION.—The explanation required under subsection (a) shall be provided in a manner that is understandable to a reasonable person and shall avoid technical jargon or overly complex language.

SEC. 521. RIGHT TO HUMAN REVIEW.

(a) IN GENERAL.—An individual who is subject to a consequential decision made or materially supported by a covered algorithm has the right to request human review of the decision.

(b) REVIEW PROCESS.—Upon receiving a request for human review, the covered entity shall:

(1) provide the individual with an opportunity to present additional information relevant to the decision;

(2) assign a qualified human decision-maker to review the algorithmic decision and any additional information provided by the individual;

(3) ensure that the human reviewer has the authority to override or modify the algorithmic decision;

(4) communicate the outcome of the review to the individual, including an explanation of how any additional information was considered;

(5) complete the review process within 30 days of receiving the request, or such other period as the Administrator may establish by regulation.

CHAPTER 4 - CHILDREN'S ONLINE SAFETY

SEC. 530. CHILDREN'S ONLINE SAFETY REQUIREMENTS.

(a) PROHIBITION ON TARGETED ADVERTISING TO CHILDREN.—A covered platform shall not engage in targeted advertising directed to a user that the covered platform knows or should know is a child.

(b) PROHIBITION ON PERSONAL DATA COLLECTION FROM CHILDREN.—Except as necessary to provide the service, a covered platform shall not collect, process, or retain personal data of a user that the covered platform knows or should know is a child without verifiable parental consent.

(c) DESIGN REQUIREMENTS.—A covered platform shall design its products and services used by children to:

(1) minimize features that may be harmful to children, including features designed to maximize engagement or create compulsive usage patterns;

(2) provide age-appropriate default privacy settings;

(3) limit contact from strangers and adults unknown to the child;

(4) restrict the recommendation of potentially harmful content;

(5) provide parental controls and oversight tools.

(d) DUTY OF CARE.—A covered platform has a duty of care to act in the best interests of users who are minors and to prevent and mitigate harms to minors arising from use of the platform.

TITLE VI - SUSTAINABLE TECHNOLOGY DEVELOPMENT

CHAPTER 1 - GREEN TECHNOLOGY RESEARCH

SEC. 601. GREEN TECHNOLOGY RESEARCH AND DEVELOPMENT.

(a) IN GENERAL.—The Secretary of Energy shall establish a program to support research, development, and demonstration of green technologies that reduce environmental impacts of the technology sector.

(b) PRIORITY AREAS.—The program shall prioritize research in:

(1) energy-efficient computing, including neuromorphic computing, quantum computing, and other advanced computing paradigms;

(2) sustainable data center design and operation, including cooling technologies, power management, and renewable energy integration;

(3) carbon capture and utilization technologies applicable to the technology sector;

(4) sustainable materials for electronics manufacturing;

(5) energy harvesting technologies for IoT devices and sensors;

(6) life cycle assessment methodologies for digital technologies;

(7) technologies for electronic waste reduction and recycling.

CHAPTER 2 - TECHNOLOGY ENVIRONMENTAL STANDARDS

SEC. 610. DATA CENTER ENERGY EFFICIENCY.

(a) EFFICIENCY STANDARDS.—Not later than 2 years after the date of enactment of this Act, the Administrator shall establish energy efficiency standards for data centers operated by covered entities.

(b) STANDARD ELEMENTS.—The standards established under subsection (a) shall address:

(1) power usage effectiveness (PUE) metrics and targets;

(2) water usage effectiveness for cooling systems;

(3) renewable energy procurement and usage;

(4) server utilization and virtualization requirements;

(5) waste heat recovery and utilization;

(6) measurement, reporting, and verification procedures.

SEC. 611. AI ENERGY AND ENVIRONMENTAL REPORTING.

(a) REPORTING REQUIREMENT.—Developers of foundation models and frontier AI systems shall report to the Administrator information regarding the energy consumption and carbon footprint of model training and operation.

(b) REPORT CONTENTS.—Reports required under subsection (a) shall include:

(1) the total computing resources used for model training;

(2) estimated energy consumption for model training;

(3) estimated carbon emissions associated with model training and operation;

(4) the location of computing facilities used and their energy sources;

(5) steps taken to reduce the environmental impact of model development and deployment.

CHAPTER 3 - CIRCULAR ECONOMY INITIATIVES

SEC. 620. ELECTRONIC WASTE REDUCTION.

(a) EXTENDED PRODUCER RESPONSIBILITY.—Manufacturers of covered electronic devices shall be responsible for the collection, recycling, and proper disposal of such devices at the end of their useful life.

(b) RIGHT TO REPAIR.—

(1) IN GENERAL.—Manufacturers of covered electronic devices shall make available to independent repair providers and consumers, on fair and reasonable terms: (A) parts and tools necessary for repair; (B) documentation, including diagnostic tools, service manuals, and schematic diagrams; and (C) software updates necessary to maintain device functionality.

(2) EXCEPTION.—The requirements of paragraph (1) shall not apply to information or tools that would compromise security features designed to prevent unauthorized access to the device or that would enable circumvention of digital rights management protections.

TITLE VII - INNOVATION AND COMPETITIVENESS

CHAPTER 1 - RESEARCH AND DEVELOPMENT PROGRAMS

SEC. 701. NATIONAL TECHNOLOGY RESEARCH PROGRAM.

(a) ESTABLISHMENT.—There is established the National Technology Research Program within the Department of Commerce to support fundamental and applied research in emerging technologies.

(b) RESEARCH PRIORITIES.—The Program shall prioritize research in:

(1) artificial intelligence and machine learning, including AI safety, alignment, and interpretability;

(2) quantum information science, including quantum computing, communications, and sensing;

(3) advanced materials, including semiconductors and nanotechnology;

(4) biotechnology and biomanufacturing;

(5) clean energy technologies;

(6) advanced networking and communications, including 6G technologies;

(7) cybersecurity and privacy-enhancing technologies;

(8) human-computer interaction and extended reality.

SEC. 702. NATIONAL AI RESEARCH INSTITUTES.

(a) ESTABLISHMENT.—The Director of the National Science Foundation shall establish a network of National AI Research Institutes to conduct fundamental research, develop AI talent, and promote collaboration across sectors.

(b) INSTITUTE FUNCTIONS.—Each National AI Research Institute shall:

(1) conduct research addressing fundamental questions in AI science and engineering;

(2) develop and disseminate educational curricula and training programs;

(3) facilitate collaboration between academia, industry, government, and civil society;

(4) develop shared research infrastructure and datasets;

(5) translate research into applications benefiting society;

(6) address ethical, social, and policy implications of AI technologies.

CHAPTER 2 - TECHNOLOGY TRANSFER

SEC. 710. TECHNOLOGY TRANSFER ENHANCEMENT.

(a) IN GENERAL.—Federal agencies shall take steps to accelerate the transfer of federally funded research and technology to the private sector for commercialization.

(b) MEASURES.—To accomplish the goal set forth in subsection (a), Federal agencies shall:

(1) streamline processes for licensing federally owned intellectual property;

(2) establish programs to connect researchers with entrepreneurs and investors;

(3) provide funding for proof-of-concept research and technology validation;

(4) support the formation of startup companies based on federally funded research;

(5) develop metrics for measuring technology transfer success.

CHAPTER 3 - INTERNATIONAL COOPERATION

SEC. 720. INTERNATIONAL TECHNOLOGY PARTNERSHIPS.

(a) POLICY.—It is the policy of the United States to pursue international cooperation on emerging technology governance with like-minded partners and allies while protecting national security interests.

(b) AREAS OF COOPERATION.—The Secretary of State, in coordination with other relevant agencies, shall pursue international cooperation in the following areas:

(1) development of common standards and principles for AI governance;

(2) coordination on export controls for sensitive technologies;

(3) joint research and development programs;

(4) sharing of best practices for technology policy;

(5) coordination on cybersecurity threats and incident response;

(6) harmonization of privacy and data protection frameworks;

(7) joint initiatives to address misuse of technology by authoritarian regimes.

TITLE VIII - WORKFORCE DEVELOPMENT

CHAPTER 1 - TECHNOLOGY EDUCATION PROGRAMS

SEC. 801. STEM AND TECHNOLOGY EDUCATION.

(a) GRANTS.—The Secretary of Education shall award grants to State educational agencies, local educational agencies, and institutions of higher education to expand and improve STEM and technology education programs.

(b) AUTHORIZED ACTIVITIES.—Grant funds under this section may be used for:

(1) developing and implementing computer science and AI literacy curricula;

(2) training teachers in technology subjects;

(3) providing technology equipment and infrastructure for schools;

(4) supporting extracurricular technology programs and competitions;

(5) developing partnerships between schools and technology employers;

(6) programs to increase participation of underrepresented groups in technology fields.

CHAPTER 2 - APPRENTICESHIP AND TRAINING

SEC. 810. TECHNOLOGY APPRENTICESHIP PROGRAM.

(a) ESTABLISHMENT.—The Secretary of Labor shall establish a national technology apprenticeship program to provide individuals with on-the-job training and related instruction in technology fields.

(b) PROGRAM ELEMENTS.—The program shall include:

(1) standards for registered technology apprenticeships;

(2) grants to employers and industry associations to develop apprenticeship programs;

(3) support for community colleges and technical schools to provide related instruction;

(4) mechanisms for awarding credentials and certifications;

(5) outreach to underrepresented populations.

CHAPTER 3 - DISPLACED WORKER ASSISTANCE

SEC. 820. TECHNOLOGY TRANSITION ASSISTANCE.

(a) ESTABLISHMENT.—The Secretary of Labor shall establish a Technology Transition Assistance program to provide support to workers displaced by technological change, including automation and AI-driven productivity improvements.

(b) ELIGIBILITY.—A worker is eligible for assistance under this section if the worker has been separated from employment due to automation, artificial intelligence implementation, or other technological changes that eliminated the worker's position.

(c) BENEFITS.—Eligible workers may receive:

(1) income support during retraining;

(2) tuition assistance for education and training programs;

(3) career counseling and job placement services;

(4) relocation assistance;

(5) health insurance subsidies during transition.

TITLE IX - ENFORCEMENT AND COMPLIANCE

CHAPTER 1 - REGULATORY FRAMEWORK

SEC. 901. NATIONAL TECHNOLOGY GOVERNANCE ADMINISTRATION.

(a) ESTABLISHMENT.—There is established within the Department of Commerce an agency to be known as the National Technology Governance Administration.

(b) ADMINISTRATOR.—The Administration shall be headed by an Administrator, who shall be appointed by the President, by and with the advice and consent of the Senate.

(c) FUNCTIONS.—The Administration shall:

(1) develop and implement regulations under this Act;

(2) conduct oversight and enforcement activities;

(3) develop technical standards and guidance;

(4) coordinate with other Federal agencies on technology policy;

(5) provide guidance to covered entities on compliance;

(6) conduct research and analysis on emerging technology issues;

(7) engage with international partners on technology governance;

(8) submit annual reports to Congress on the state of technology governance.

SEC. 902. RULEMAKING AUTHORITY.

(a) IN GENERAL.—The Administrator shall have authority to promulgate rules and regulations necessary to implement and enforce this Act.

(b) NOTICE AND COMMENT.—Any rule promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code.

(c) PERIODIC REVIEW.—Not less frequently than every 4 years, the Administrator shall conduct a review of regulations promulgated under this Act to determine whether such regulations remain appropriate in light of technological developments and other relevant factors.

CHAPTER 2 - CIVIL PENALTIES

SEC. 910. CIVIL PENALTIES.

(a) IN GENERAL.—Any covered entity that violates any provision of this Act or any regulation promulgated thereunder shall be liable for a civil penalty in an amount not to exceed:

(1) for violations of Title III (Artificial Intelligence Governance), the greater of: (A) $50,000 per violation; or (B) 4 percent of the covered entity's global annual revenue for the preceding fiscal year;

(2) for violations of Title V (Digital Rights and Privacy), the greater of: (A) $50,000 per violation or $100 per affected individual; or (B) 4 percent of the covered entity's global annual revenue for the preceding fiscal year;

(3) for violations of Title IV (Cybersecurity Enhancement), the greater of: (A) $100,000 per violation; or (B) 2 percent of the covered entity's global annual revenue for the preceding fiscal year;

(4) for other violations, $25,000 per violation.

(b) FACTORS.—In determining the amount of a civil penalty under this section, the Administrator or the Commission, as applicable, shall consider:

(1) the nature, circumstances, extent, and gravity of the violation;

(2) the degree of culpability of the violator;

(3) any history of prior violations;

(4) the ability of the violator to pay;

(5) the effect of the penalty on the ability of the violator to continue doing business;

(6) the economic benefit gained by the violator from the violation;

(7) efforts by the violator to remedy the violation and prevent future violations;

(8) cooperation with enforcement authorities.

SEC. 911. ENFORCEMENT BY THE COMMISSION.

(a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of any provision of Title V of this Act or any regulation promulgated thereunder 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)).

(b) POWERS OF THE COMMISSION.—The Commission shall enforce this Act and the regulations promulgated thereunder in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

CHAPTER 3 - CRIMINAL PENALTIES

SEC. 920. CRIMINAL PENALTIES.

(a) KNOWING VIOLATIONS.—Any person who knowingly violates any provision of this Act or any regulation promulgated thereunder, with intent to defraud or cause harm, shall be fined not more than $250,000, imprisoned not more than 5 years, or both.

(b) AGGRAVATED VIOLATIONS.—Any person who commits an aggravated violation of this Act shall be fined not more than $1,000,000, imprisoned not more than 10 years, or both. For purposes of this subsection, an 'aggravated violation' means a knowing violation that:

(1) results in bodily injury or death;

(2) affects more than 1,000,000 individuals;

(3) involves the data of children;

(4) constitutes a pattern or practice of violations;

(5) is committed by a person who has previously been convicted of a violation of this Act.

CHAPTER 4 - JUDICIAL REVIEW

SEC. 930. JUDICIAL REVIEW.

(a) RIGHT OF REVIEW.—Any person aggrieved by a final order of the Administrator or the Commission under this Act may obtain review of such order in the United States Court of Appeals for the circuit in which such person resides or has its principal place of business, or in the United States Court of Appeals for the District of Columbia Circuit.

(b) FILING.—A petition for review must be filed within 60 days after the date on which the final order was issued.

(c) STANDARD OF REVIEW.—The court shall hold unlawful and set aside the order of the Administrator or the Commission if the order is: (1) arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law; (2) contrary to constitutional right, power, privilege, or immunity; (3) in excess of statutory jurisdiction, authority, or limitations; or (4) unsupported by substantial evidence.

SEC. 931. PRIVATE RIGHT OF ACTION.

(a) IN GENERAL.—Any individual who suffers an injury as a result of a violation of Title V of this Act may bring a civil action in any court of competent jurisdiction against the covered entity that committed the violation.

(b) RELIEF.—In an action under this section, the court may award:

(1) actual damages, but not less than $100 and not more than $1,000 per violation;

(2) punitive damages in cases of willful or reckless violations;

(3) injunctive or declaratory relief;

(4) reasonable attorney's fees and costs.

(c) STATUTE OF LIMITATIONS.—An action under this section may not be commenced later than 4 years after the date on which the violation occurred or the date on which the individual discovered or should have discovered the violation, whichever is later.

TITLE X - APPROPRIATIONS AND FUNDING

CHAPTER 1 - AUTHORIZATION OF APPROPRIATIONS

SEC. 1001. AUTHORIZATION OF APPROPRIATIONS.

(a) NATIONAL TECHNOLOGY GOVERNANCE ADMINISTRATION.—There are authorized to be appropriated to the National Technology Governance Administration:

(1) $500,000,000 for fiscal year 2025;

(2) $600,000,000 for fiscal year 2026;

(3) $700,000,000 for fiscal year 2027;

(4) $800,000,000 for fiscal year 2028; and

(5) $900,000,000 for fiscal year 2029.

(b) INFRASTRUCTURE MODERNIZATION.—There are authorized to be appropriated for infrastructure modernization programs under Title II:

(1) $10,000,000,000 for fiscal year 2025;

(2) $12,000,000,000 for fiscal year 2026;

(3) $14,000,000,000 for fiscal year 2027;

(4) $16,000,000,000 for fiscal year 2028; and

(5) $18,000,000,000 for fiscal year 2029.

(c) CYBERSECURITY.—There are authorized to be appropriated for cybersecurity programs under Title IV:

(1) $2,000,000,000 for fiscal year 2025;

(2) $2,500,000,000 for fiscal year 2026;

(3) $3,000,000,000 for fiscal year 2027;

(4) $3,500,000,000 for fiscal year 2028; and

(5) $4,000,000,000 for fiscal year 2029.

(d) RESEARCH AND DEVELOPMENT.—There are authorized to be appropriated for research and development programs under Title VII:

(1) $5,000,000,000 for fiscal year 2025;

(2) $6,000,000,000 for fiscal year 2026;

(3) $7,000,000,000 for fiscal year 2027;

(4) $8,000,000,000 for fiscal year 2028; and

(5) $9,000,000,000 for fiscal year 2029.

(e) WORKFORCE DEVELOPMENT.—There are authorized to be appropriated for workforce development programs under Title VIII:

(1) $1,000,000,000 for fiscal year 2025;

(2) $1,200,000,000 for fiscal year 2026;

(3) $1,400,000,000 for fiscal year 2027;

(4) $1,600,000,000 for fiscal year 2028; and

(5) $1,800,000,000 for fiscal year 2029.

CHAPTER 2 - GRANT PROGRAMS

SEC. 1010. STATE AND LOCAL TECHNOLOGY GRANTS.

(a) ESTABLISHMENT.—The Administrator shall establish a grant program to assist State, local, Tribal, and territorial governments in implementing the requirements of this Act and developing technology capacity.

(b) ELIGIBLE USES.—Grant funds under this section may be used for:

(1) development of State and local data privacy programs;

(2) implementation of cybersecurity measures for State and local government systems;

(3) assessment and remediation of AI systems used by State and local governments;

(4) workforce development and training for State and local government employees;

(5) public engagement and education on technology issues;

(6) development of digital equity programs.

CHAPTER 3 - FUNDING ALLOCATIONS

SEC. 1020. ALLOCATION OF FUNDS.

(a) INFRASTRUCTURE FUNDS.—Of the amounts appropriated under section 1001(b):

(1) 40 percent shall be for broadband infrastructure programs under sections 210-212;

(2) 25 percent shall be for transportation infrastructure programs under sections 220-221;

(3) 20 percent shall be for energy infrastructure programs under sections 230-231;

(4) 15 percent shall be for water infrastructure programs under sections 240.

(b) RESEARCH FUNDS.—Of the amounts appropriated under section 1001(d):

(1) 35 percent shall be for AI research programs;

(2) 20 percent shall be for quantum computing research;

(3) 15 percent shall be for cybersecurity research;

(4) 15 percent shall be for clean energy technology research;

(5) 15 percent shall be for other emerging technology research.

TITLE XI - IMPLEMENTATION AND EFFECTIVE DATES

CHAPTER 1 - IMPLEMENTATION SCHEDULE

SEC. 1101. EFFECTIVE DATES.

(a) GENERAL EFFECTIVE DATE.—Except as otherwise provided in this section, this Act shall take effect on the date of enactment.

(b) TITLE III (AI GOVERNANCE).—

(1) The prohibition on unacceptable risk AI systems under section 301(b)(1) shall take effect 180 days after the date of enactment.

(2) The requirements for high-risk AI systems under Chapter 2 of Title III shall take effect 2 years after the date of enactment.

(3) The transparency requirements under Chapter 3 of Title III shall take effect 1 year after the date of enactment.

(c) TITLE V (DIGITAL RIGHTS AND PRIVACY).—

(1) For large covered entities, the requirements of Title V shall take effect 1 year after the date of enactment.

(2) For small businesses, the requirements of Title V shall take effect 2 years after the date of enactment.

(d) CYBERSECURITY REQUIREMENTS.—The cybersecurity requirements under Title IV shall take effect 18 months after the date of enactment.

SEC. 1102. RULEMAKING DEADLINES.

(a) PRIORITY RULEMAKINGS.—Not later than 1 year after the date of enactment of this Act, the Administrator shall promulgate final rules implementing:

(1) the AI risk classification framework under section 301;

(2) the requirements for high-risk AI systems under section 310;

(3) the algorithmic impact assessment requirements under section 330;

(4) the consumer data rights under section 501.

(b) OTHER RULEMAKINGS.—Not later than 2 years after the date of enactment of this Act, the Administrator shall promulgate final rules implementing all other provisions of this Act requiring rulemaking.

CHAPTER 2 - TRANSITION PROVISIONS

SEC. 1110. TRANSITION PERIOD.

(a) EXISTING AI SYSTEMS.—AI systems that are on the market or in service as of the date of enactment of this Act shall be brought into compliance with the requirements of Title III within 3 years of such date.

(b) EXISTING DATA PRACTICES.—Covered entities shall bring their data processing practices into compliance with the requirements of Title V within the time periods specified in section 1101(c).

(c) TRANSITION ASSISTANCE.—The Administrator shall provide guidance and technical assistance to covered entities to facilitate compliance during the transition period.

CHAPTER 3 - SEVERABILITY

SEC. 1120. SEVERABILITY.

If any provision of this Act, or the application of such provision to any person or circumstance, is held to be unconstitutional, the remainder of this Act, and the application of the provisions of such to any person or circumstance, shall not be affected thereby.

APPENDIX A - TECHNICAL STANDARDS AND SPECIFICATIONS

A.1 AI SYSTEM DOCUMENTATION REQUIREMENTS

This appendix sets forth the detailed technical documentation requirements for AI systems subject to regulation under this Act.

A.1.1 System Identification and Overview

The following information shall be included:

(1) Unique system identifier and version number;

(2) Date of initial development and all subsequent versions;

(3) Names and contact information of the developer organization;

(4) Classification under the risk framework (unacceptable/high/limited/minimal);

(5) Intended purpose and use context;

(6) Target users and beneficiaries;

(7) Known limitations and contraindications.

A.1.2 Technical Architecture

Documentation of technical architecture shall include:

(1) Model type and architecture (e.g., neural network architecture, decision tree, ensemble method);

(2) Training methodology (supervised, unsupervised, reinforcement learning, etc.);

(3) Hardware requirements for training and inference;

(4) Software dependencies and versions;

(5) Data flow diagrams;

(6) Integration points with external systems;

(7) Security measures implemented.

A.1.3 Training Data Documentation

Documentation of training data shall include:

(1) Description of training datasets, including size, format, and content types;

(2) Data sources and collection methods;

(3) Data labeling processes and quality assurance measures;

(4) Demographic composition of training data, where applicable;

(5) Known biases or gaps in training data;

(6) Data preprocessing and augmentation techniques;

(7) Data retention and storage practices;

(8) Consent and authorization for data use.

A.1.4 Performance Metrics

Performance documentation shall include:

(1) Accuracy metrics appropriate to the task (e.g., precision, recall, F1 score, AUC-ROC);

(2) Performance disaggregated by relevant demographic groups;

(3) Error analysis, including types and frequencies of errors;

(4) Confidence calibration assessment;

(5) Performance in edge cases and adversarial conditions;

(6) Comparison with baseline or alternative approaches;

(7) Drift detection and monitoring procedures.

A.2 CYBERSECURITY STANDARDS

A.2.1 Access Control Requirements

Critical infrastructure operators and high-risk AI system deployers shall implement access control measures that meet or exceed the following standards:

(1) Multi-factor authentication for all privileged access;

(2) Role-based access control with principle of least privilege;

(3) Automated account provisioning and de-provisioning;

(4) Session management with automatic timeout;

(5) Logging of all access attempts, successful and unsuccessful;

(6) Regular access reviews, at least quarterly for privileged accounts;

(7) Separation of duties for critical functions.

A.2.2 Network Security Requirements

Network security measures shall include:

(1) Network segmentation to isolate critical systems;

(2) Encryption of data in transit using TLS 1.2 or higher;

(3) Intrusion detection and prevention systems;

(4) Firewall configurations following deny-by-default principles;

(5) Regular vulnerability scanning, at least monthly;

(6) Penetration testing, at least annually;

(7) Secure configuration baselines for network devices.

A.2.3 Incident Response Requirements

Incident response capabilities shall include:

(1) Documented incident response plan reviewed at least annually;

(2) Designated incident response team with defined roles and responsibilities;

(3) 24/7 monitoring capability for critical systems;

(4) Automated alerting for security events;

(5) Forensic investigation capabilities;

(6) Communication procedures for internal and external stakeholders;

(7) Post-incident review and lessons learned process;

(8) Regular tabletop exercises and simulations.

A.3 DATA PROTECTION STANDARDS

A.3.1 Encryption Standards

Data encryption shall meet the following requirements:

(1) Sensitive covered data shall be encrypted at rest using AES-256 or equivalent;

(2) Data in transit shall be encrypted using TLS 1.2 or higher;

(3) Encryption keys shall be managed according to NIST SP 800-57 guidelines;

(4) Key rotation shall occur at least annually or upon personnel changes;

(5) Hardware security modules shall be used for key storage in high-risk applications;

(6) Quantum-resistant algorithms shall be evaluated and adopted as they become standardized.

A.3.2 De-identification Standards

Data de-identification shall meet the following requirements:

(1) Expert determination method: A qualified expert using generally accepted statistical and scientific principles and methods must determine that the risk of re-identification is very small;

(2) Safe harbor method: The following identifiers must be removed: names, geographic subdivisions smaller than a State, dates (except year) related to an individual, telephone numbers, fax numbers, email addresses, Social Security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, web URLs, IP addresses, biometric identifiers, full-face photographs, and any other unique identifying number or code;

(3) Documentation of de-identification methodology and residual re-identification risk assessment;

(4) Prohibition on re-identification attempts without authorization;

(5) Technical measures to prevent re-identification through linkage with external datasets.

APPENDIX B - COMPLIANCE MATRICES AND CHECKLISTS

B.1 HIGH-RISK AI COMPLIANCE CHECKLIST

Developers and deployers of high-risk AI systems shall use the following checklist to verify compliance with the requirements of Title III, Chapter 2:

Requirement	Section	Compliant	Notes
Risk management system established	310(b)	[ ]	
Known and foreseeable risks identified	310(b)(1)	[ ]	
Risk mitigation measures implemented	310(b)(4)	[ ]	
Data governance practices established	310(c)	[ ]	
Training data quality assessed	310(c)(1)	[ ]	
Bias examination conducted	310(c)(3)	[ ]	
Bias mitigation measures implemented	310(c)(4)	[ ]	
Technical documentation prepared	310(d)	[ ]	
System description documented	310(d)(1)	[ ]	
Development process documented	310(d)(2)	[ ]	
Training data documented	310(d)(3)	[ ]	
Performance information documented	310(d)(4)	[ ]	
Instructions for use provided	310(d)(7)	[ ]	
Logging capabilities implemented	310(e)	[ ]	
Transparency requirements met	310(f)	[ ]	
Human oversight enabled	310(g)	[ ]	
Accuracy standards met	310(h)(1)	[ ]	
Robustness standards met	310(h)(2)	[ ]	
Cybersecurity standards met	310(h)(3)	[ ]	
Conformity assessment completed	311	[ ]	
Declaration of conformity prepared	311(d)	[ ]	

B.2 PRIVACY COMPLIANCE MATRIX

Covered entities shall use the following matrix to assess compliance with data protection requirements under Title V:

Data Type	Collection	Processing	Sharing	Retention	Deletion
Name/Contact	501(a)	502(b)	501(e)(1)	502(c)	501(c)
Financial	503(b)(1)	502(b)	503(b)(2)	502(c)	501(c)
Biometric	503(b)(4)	503(b)	503(b)(1)	502(c)	501(c)
Geolocation	503(b)(5)	503(b)	503(b)(1)	502(c)	501(c)
Health	503(b)(1)	503(b)	503(b)(1)	502(c)	501(c)
Children's	530(b)	530(b)	530(a)	530(b)	501(c)

APPENDIX C - REPORTING TEMPLATES AND FORMS

C.1 CYBERSECURITY INCIDENT REPORT FORM

The following template shall be used for reporting covered cybersecurity incidents under section 420:

SECTION 1: REPORTING ENTITY INFORMATION

1.1 Organization Name: _____

1.2 Primary Contact Name: _____

1.3 Contact Email: _____

1.4 Contact Phone: _____

1.5 Organization Address: _____

1.6 Industry Sector: _____

1.7 Critical Infrastructure Designation (if applicable): _____

SECTION 2: INCIDENT INFORMATION

2.1 Date of Incident Discovery: _____

2.2 Date of Incident Occurrence (if known): _____

2.3 Duration of Incident: _____

2.4 Incident Type (check all that apply):

[ ] Ransomware

[ ] Data Breach

[ ] Denial of Service

[ ] Unauthorized Access

[ ] Malware Infection

[ ] Phishing/Social Engineering

[ ] Insider Threat

[ ] Supply Chain Compromise

[ ] Other: _____

2.5 Systems Affected: _____

2.6 Data Types Affected: _____

2.7 Number of Individuals Affected (estimate): _____

2.8 Geographic Scope of Impact: _____

SECTION 3: TECHNICAL DETAILS

3.1 Attack Vector: _____

3.2 Vulnerabilities Exploited: _____

3.3 Indicators of Compromise:

IP Addresses: _____

Domain Names: _____

File Hashes: _____

Other IOCs: _____

3.4 Tactics, Techniques, and Procedures (if known): _____

3.5 Attribution (if known): _____

SECTION 4: RESPONSE AND REMEDIATION

4.1 Immediate Response Actions Taken: _____

4.2 Containment Measures: _____

4.3 Eradication Steps: _____

4.4 Recovery Status: _____

4.5 External Assistance Engaged: _____

4.6 Law Enforcement Notified: [ ] Yes [ ] No

4.7 Lessons Learned / Improvements Planned: _____

SECTION 5: RANSOM PAYMENT (IF APPLICABLE)

5.1 Ransom Demanded: [ ] Yes [ ] No

5.2 Ransom Amount Demanded: _____

5.3 Ransom Paid: [ ] Yes [ ] No

5.4 Ransom Amount Paid: _____

5.5 Payment Method: _____

5.6 Cryptocurrency Wallet Address: _____

5.7 Data/Systems Recovered After Payment: [ ] Yes [ ] No [ ] Partial

Certification: I certify that the information provided in this report is accurate and complete to the best of my knowledge.

Signature: _____ Date: _____

C.2 ALGORITHMIC IMPACT ASSESSMENT TEMPLATE

The following template shall be used for algorithmic impact assessments required under section 330:

PART I: SYSTEM OVERVIEW

I.1 System Name and Version: _____

I.2 Developer/Vendor: _____

I.3 Deploying Organization: _____

I.4 Date of Assessment: _____

I.5 Assessment Conducted By: _____

I.6 System Purpose and Intended Use: _____

I.7 Types of Decisions Made or Supported: _____

I.8 Affected Population: _____

I.9 Scale of Deployment: _____

PART II: NECESSITY AND PROPORTIONALITY

II.1 What problem is the system designed to address?

_____

II.2 Why is an algorithmic approach necessary?

_____

II.3 What alternatives were considered?

_____

II.4 How does the system's impact compare to alternatives?

_____

PART III: DATA ASSESSMENT

III.1 Data Sources Used: _____

III.2 Data Collection Methods: _____

III.3 Data Quality Assessment: _____

III.4 Representativeness of Data: _____

III.5 Known Data Limitations or Biases: _____

III.6 Data Privacy Protections: _____

PART IV: FAIRNESS AND BIAS ANALYSIS

IV.1 Fairness Metrics Used: _____

IV.2 Performance Across Demographic Groups:

Overall Accuracy: _____

False Positive Rates by Group: _____

False Negative Rates by Group: _____

IV.3 Identified Disparities: _____

IV.4 Root Cause Analysis: _____

IV.5 Mitigation Measures: _____

IV.6 Residual Disparities After Mitigation: _____

PART V: RISK ASSESSMENT

V.1 Potential Harms Identified:

[ ] Physical harm

[ ] Psychological harm

[ ] Financial harm

[ ] Reputational harm

[ ] Denial of opportunity

[ ] Privacy violation

[ ] Discrimination

[ ] Other: _____

V.2 Likelihood of Each Harm (Low/Medium/High): _____

V.3 Severity of Each Harm (Low/Medium/High): _____

V.4 Risk Mitigation Measures: _____

PART VI: HUMAN OVERSIGHT

VI.1 Level of Automation: _____

VI.2 Human Review Procedures: _____

VI.3 Override Capabilities: _____

VI.4 Training for Human Reviewers: _____

VI.5 Performance Monitoring: _____

PART VII: TRANSPARENCY AND CONTESTABILITY

VII.1 Notice Provided to Affected Individuals: _____

VII.2 Explanation Capability: _____

VII.3 Appeal/Contest Procedures: _____

VII.4 Response Time for Appeals: _____

PART VIII: ONGOING MONITORING

VIII.1 Performance Monitoring Plan: _____

VIII.2 Drift Detection Procedures: _____

VIII.3 Periodic Review Schedule: _____

VIII.4 Update and Retraining Procedures: _____

Certification: I certify that this algorithmic impact assessment has been conducted in accordance with the requirements of section 330 and that the information provided is accurate and complete to the best of my knowledge.

Signature: _____ Date: _____

Title: _____

Passed the House of Representatives [DATE]

_____

Clerk of the House of Representatives

Passed the Senate [DATE]

_____

Secretary of the Senate

APPENDIX D - SECTOR-SPECIFIC REQUIREMENTS

D.1 HEALTHCARE SECTOR AI REQUIREMENTS

This section establishes specific requirements for artificial intelligence systems deployed in healthcare settings, including but not limited to clinical decision support systems, diagnostic tools, treatment recommendation systems, and administrative AI applications.

D.1.1 Clinical Decision Support Systems

Clinical decision support (CDS) systems that use artificial intelligence to analyze patient data and provide recommendations to healthcare providers shall comply with the following additional requirements:

(1) Clinical validation shall be conducted using diverse patient populations representative of the intended deployment setting, including appropriate representation of race, ethnicity, sex, age, and comorbidity profiles;

(2) Performance metrics shall be reported separately for each major demographic subgroup, with particular attention to historically underserved populations that may be underrepresented in training data;

(3) The system shall clearly indicate the confidence level associated with each recommendation and the key factors contributing to the recommendation in a manner understandable to clinicians;

(4) Override rates and clinical outcomes following system recommendations shall be tracked and reported to enable ongoing performance assessment;

(5) Systems shall be designed to integrate with existing clinical workflows without creating alert fatigue or imposing excessive cognitive burden on healthcare providers;

(6) Clear disclaimers shall be provided indicating that AI recommendations are advisory and do not replace clinical judgment;

(7) Systems shall maintain compatibility with applicable health information technology standards, including HL7 FHIR and relevant clinical terminology standards;

(8) Training data provenance shall be documented, including institutional sources, date ranges, and any known biases or limitations in the underlying datasets;

(9) Systems making recommendations regarding controlled substances shall include appropriate safeguards against misuse consistent with applicable regulations;

(10) Post-market surveillance shall be conducted to identify performance degradation, emerging biases, or unexpected adverse outcomes.

D.1.2 Diagnostic AI Systems

AI systems used for medical diagnosis, including but not limited to radiology, pathology, dermatology, and ophthalmology applications, shall meet the following requirements:

(1) Sensitivity and specificity shall be reported for each intended diagnostic indication, with separate reporting for different disease severities and stages where applicable;

(2) The system shall clearly communicate uncertainty and limitations, including cases where the AI system cannot provide a reliable assessment;

(3) Mechanisms shall be implemented to detect and flag cases that fall outside the system's validated performance envelope;

(4) The system shall be validated on external datasets independent from training data to assess generalization capability;

(5) Image or data quality requirements shall be clearly documented, with the system capable of rejecting inputs that do not meet quality thresholds;

(6) For systems intended to operate autonomously, additional safety mechanisms shall be implemented, including second-read requirements for findings above specified severity thresholds;

(7) The system shall maintain audit logs sufficient to support retrospective analysis of diagnostic performance;

(8) Radiomics or other quantitative imaging features used by the system shall be documented with evidence of reproducibility and clinical relevance;

(9) For pathology applications, the system shall account for variations in tissue preparation, staining protocols, and scanner characteristics across different laboratory settings;

(10) Regular calibration and quality assurance protocols shall be established and documented.

D.1.3 Healthcare Administrative AI

AI systems used for healthcare administrative functions, including prior authorization, claims processing, provider credentialing, and resource allocation, shall comply with:

(1) Prior authorization systems shall provide clear explanations for coverage determinations, including specific clinical criteria applied and documentation considered;

(2) Appeal mechanisms shall be established allowing healthcare providers and patients to request human review of automated decisions;

(3) Systems shall not create systematic barriers to care that disproportionately affect patients based on race, ethnicity, disability status, or other protected characteristics;

(4) Processing times shall be monitored to ensure automated systems do not create delays compared to human review processes;

(5) Systems used for fraud, waste, and abuse detection shall be designed to minimize false positives that could inappropriately burden legitimate healthcare providers;

(6) Resource allocation systems shall incorporate explicit consideration of health equity and access to care for underserved populations;

(7) Documentation requirements shall be reasonable and shall not impose excessive administrative burden on healthcare providers.

D.2 FINANCIAL SERVICES SECTOR REQUIREMENTS

This section establishes specific requirements for artificial intelligence systems deployed in financial services, including credit underwriting, insurance pricing, fraud detection, algorithmic trading, and customer service applications.

D.2.1 Credit Underwriting and Lending

AI systems used in credit underwriting, lending decisions, or credit scoring shall comply with the following requirements in addition to existing fair lending laws:

(1) Adverse action notices shall include the specific factors that contributed to the decision in a manner understandable to the applicant, consistent with requirements of the Equal Credit Opportunity Act and Fair Credit Reporting Act;

(2) Regular testing shall be conducted to identify discriminatory impacts, including disparate treatment and disparate impact on the basis of race, color, religion, national origin, sex, marital status, age, receipt of public assistance, or exercise of rights under the Consumer Credit Protection Act;

(3) Alternative data sources used in credit decisions shall be documented and validated for predictive validity and lack of discriminatory proxy effects;

(4) Model risk management practices shall be consistent with applicable regulatory guidance, including OCC Bulletin 2011-12 and related supervisory expectations;

(5) Systems shall be capable of providing individualized explanations sufficient to enable applicants to understand and potentially improve their creditworthiness;

(6) Documentation shall be maintained sufficient to demonstrate compliance with fair lending requirements and enable regulatory examination;

(7) Third-party models shall be subject to appropriate due diligence and ongoing monitoring by the financial institution;

(8) Feedback loops that could perpetuate historical discrimination shall be identified and mitigated.

D.2.2 Insurance Underwriting and Pricing

AI systems used in insurance underwriting, pricing, or claims processing shall comply with:

(1) Rating factors derived from AI systems shall be actuarially justified and shall not constitute unfair discrimination prohibited under applicable state insurance laws;

(2) Explanation capabilities shall enable insurance companies to respond to regulatory inquiries regarding the basis for premium determinations;

(3) Systems used in claims processing shall provide clear explanations for claim denials and shall not create systematic barriers to legitimate claims;

(4) The use of external data sources shall be disclosed to consumers and shall comply with applicable insurance information practices acts;

(5) Life and health insurance applications shall comply with genetic information non-discrimination requirements;

(6) Systems shall be tested for compliance with state unfair trade practices statutes;

(7) Marketing and customer segmentation systems shall not engage in unfair discrimination in the availability of insurance;

(8) Regular audits shall be conducted to ensure pricing outcomes remain actuarially sound and non-discriminatory over time.

D.2.3 Algorithmic Trading Systems

AI systems used in securities trading, market making, or investment management shall comply with:

(1) Risk management controls shall be implemented to prevent excessive market impact, including position limits, loss limits, and circuit breakers;

(2) Systems shall be tested under stressed market conditions and extreme scenarios to assess potential for destabilizing behavior;

(3) Audit trails shall be maintained sufficient to reconstruct trading decisions and demonstrate compliance with market manipulation prohibitions;

(4) Systems shall be designed to detect and prevent potential market manipulation, including spoofing, layering, and wash trading;

(5) Best execution obligations shall be monitored and documented;

(6) Conflicts of interest between proprietary trading and customer order handling shall be identified and managed;

(7) Model governance and change management procedures shall be documented and followed;

(8) Regular testing shall verify that trading algorithms operate as intended and within established risk parameters.

D.3 EMPLOYMENT SECTOR REQUIREMENTS

This section establishes specific requirements for artificial intelligence systems used in employment contexts, including recruiting, hiring, performance evaluation, promotion, compensation, task allocation, and termination decisions.

D.3.1 Automated Employment Decision Tools

Automated employment decision tools that substantially assist or replace discretionary decision making in employment shall comply with the following requirements:

(1) Bias audits shall be conducted annually by independent auditors to assess disparate impact on the basis of race, ethnicity, sex, and other protected characteristics;

(2) Summary audit results shall be made publicly available and shall include impact ratios for each protected group;

(3) Job seekers and employees shall receive notice prior to the use of automated employment decision tools, including information about how to request an alternative selection process or reasonable accommodation;

(4) Tools shall be validated for job-relatedness and business necessity, with validation studies documented and available for regulatory review;

(5) Scoring or ranking methodologies shall be transparent, with clear documentation of the factors considered and their relative weights;

(6) Candidates shall have the opportunity to request information about the basis for adverse decisions and to provide additional information for consideration;

(7) Video interview analysis tools shall comply with applicable disability discrimination requirements and provide reasonable accommodations;

(8) Personality assessments and other indirect measures shall be validated for predictive validity and lack of adverse impact;

(9) Continuous monitoring shall be conducted to identify performance degradation or emerging disparities in deployment;

(10) Data retention practices shall comply with applicable recordkeeping requirements under Title VII and related regulations.

D.3.2 Workplace Monitoring Systems

AI systems used for workplace monitoring, productivity tracking, or performance evaluation shall comply with the following requirements:

(1) Employees shall receive clear notice of monitoring practices, including the types of data collected, purposes of collection, and how data will be used in employment decisions;

(2) Monitoring shall be proportionate to legitimate business needs and shall minimize intrusion into employee privacy;

(3) Keystroke logging, screen capture, webcam monitoring, and similar invasive monitoring techniques shall be used only when necessary for specific legitimate purposes and shall not be used for general productivity tracking;

(4) Systems that score or rank employee productivity shall provide employees with access to their data and the methodology used in scoring;

(5) Algorithmic management systems shall not be designed to create unsustainable work pace or unsafe working conditions;

(6) Systems shall include mechanisms to account for legitimate variations in productivity, including disability accommodations, breaks, and non-productive work time;

(7) Location tracking of employees shall be limited to work hours and work-related purposes;

(8) Biometric time tracking systems shall provide alternative options for employees who object on religious or personal grounds.

D.4 EDUCATION SECTOR REQUIREMENTS

This section establishes specific requirements for artificial intelligence systems used in educational settings, including admissions, grading, learning management, proctoring, and student support systems.

D.4.1 Admissions and Academic Assessment

AI systems used in admissions decisions or academic assessment shall comply with:

(1) Systems shall be validated for reliability, validity, and lack of bias against students from different demographic backgrounds, socioeconomic circumstances, or educational settings;

(2) Automated essay scoring systems shall be transparent about the factors evaluated and shall be validated against human scoring standards;

(3) Systems shall account for legitimate variations in student circumstances, including disability status, English language learner status, and access to educational resources;

(4) Students and parents shall have the right to request human review of automated academic assessments that have significant impact on educational opportunities;

(5) Proctoring systems shall minimize false accusations and shall provide clear processes for challenging automated misconduct determinations;

(6) Data collected by educational AI systems shall be used only for educational purposes and shall not be sold or shared for commercial purposes unrelated to the educational mission;

(7) Predictive systems identifying students at risk of academic difficulty shall be designed to support student success rather than to exclude students from opportunities;

(8) Systems shall comply with the Family Educational Rights and Privacy Act (FERPA) and other applicable student privacy laws.

D.4.2 Learning Management and Adaptive Systems

AI-powered learning management and adaptive learning systems shall comply with:

(1) Adaptive learning systems shall be validated for effectiveness across diverse student populations;

(2) Personalization algorithms shall be transparent to educators and shall not inappropriately limit student exposure to curriculum content;

(3) Systems shall be designed to promote student agency and shall not create dependency on algorithmic guidance;

(4) Student behavioral data collected by learning systems shall be subject to data minimization principles;

(5) Teachers shall retain meaningful oversight and control over AI-assisted instruction;

(6) Systems shall provide mechanisms for students and educators to understand and contest algorithmic recommendations;

(7) Gamification and engagement features shall be designed to promote genuine learning rather than addictive behavior patterns.

D.5 HOUSING SECTOR REQUIREMENTS

This section establishes specific requirements for artificial intelligence systems used in housing, including tenant screening, rental pricing, property advertising, and housing assistance determinations.

D.5.1 Tenant Screening Systems

AI systems used for tenant screening shall comply with the following requirements:

(1) Tenant screening systems shall comply with the Fair Housing Act and shall not discriminate on the basis of race, color, national origin, religion, sex, familial status, or disability;

(2) Systems shall be tested for disparate impact and shall be validated for accuracy and predictive validity;

(3) Criminal history information shall be used in accordance with HUD guidance on criminal records screening;

(4) Adverse action notices shall provide specific reasons for denial and information about how to dispute inaccurate information;

(5) Systems shall provide mechanisms for applicants to explain or provide context for negative information;

(6) Scoring methodologies shall be documented and shall use only factors with demonstrated relevance to tenancy outcomes;

(7) Income requirements and algorithms shall not create unjustified barriers for applicants receiving housing assistance or with non-traditional income sources;

(8) Systems shall be monitored for steering effects that may result in discriminatory housing patterns.

D.5.2 Rental Pricing Algorithms

AI systems used for rental pricing optimization shall comply with:

(1) Pricing algorithms shall not facilitate collusion or coordination of rental prices in violation of antitrust laws;

(2) Systems shall not use protected characteristics or proxies for protected characteristics in pricing determinations;

(3) Dynamic pricing practices shall be transparent to consumers;

(4) Systems shall be designed to avoid exacerbating housing affordability crises in local markets;

(5) Fair housing testing shall be conducted to ensure pricing outcomes do not vary impermissibly based on protected characteristics.

APPENDIX E - INTERNATIONAL STANDARDS CROSS-REFERENCE

E.1 MAPPING TO EU AI ACT

This appendix provides a cross-reference between the requirements of this Act and the corresponding provisions of the European Union Artificial Intelligence Act (EU AI Act) to facilitate compliance by organizations operating in multiple jurisdictions.

This Act	EU AI Act	Topic
Sec. 301(b)(1)	Art. 5	Prohibited AI practices
Sec. 301(b)(2)	Art. 6	High-risk classification
Sec. 310(b)	Art. 9	Risk management system
Sec. 310(c)	Art. 10	Data governance
Sec. 310(d)	Art. 11	Technical documentation
Sec. 310(e)	Art. 12	Record-keeping
Sec. 310(f)	Art. 13	Transparency
Sec. 310(g)	Art. 14	Human oversight
Sec. 310(h)	Art. 15	Accuracy and security
Sec. 311	Art. 43	Conformity assessment
Sec. 320(a)	Art. 52(1)	AI interaction disclosure
Sec. 320(b)	Art. 52(3)	Deepfake labeling
Sec. 341	Art. 52c	Foundation models

E.2 MAPPING TO ISO/IEC STANDARDS

The following table maps the requirements of this Act to relevant ISO/IEC standards for artificial intelligence:

This Act Section	ISO/IEC Standard	Standard Title
Sec. 301	ISO/IEC 22989:2022	AI concepts and terminology
Sec. 310(b)	ISO/IEC 23894:2023	AI risk management
Sec. 310(c)	ISO/IEC 5259:2024	Data quality for analytics and AI
Sec. 310(h)	ISO/IEC 24029	Assessment of robustness of neural networks
Sec. 320	ISO/IEC TR 24028:2020	Trustworthiness in AI

Sec. 330	ISO/IEC TR 24027:2021	Bias in AI systems
Sec. 340	ISO/IEC 42001:2023	AI management system
Title IV	ISO/IEC 27001:2022	Information security management
Title V	ISO/IEC 27701:2019	Privacy information management

E.3 MAPPING TO NIST AI RISK MANAGEMENT FRAMEWORK

This section maps the requirements of this Act to the NIST AI Risk Management Framework:

This Act	NIST AI RMF	Function/Category
Sec. 104	Govern 1.1-1.7	Organizational governance
Sec. 301	Map 1.1-1.6	Context and risk identification
Sec. 310(b)	Map 2.1-2.3	AI risk assessment
Sec. 310(c)	Map 3.1-3.5	AI lifecycle considerations
Sec. 310(d)	Govern 4.1-4.3	Documentation practices
Sec. 310(f)	Manage 2.1-2.4	Transparency mechanisms
Sec. 310(g)	Manage 3.1-3.2	Human oversight
Sec. 320	Measure 2.1-2.13	Trustworthiness measurement
Sec. 330	Manage 4.1-4.3	Impact assessment
Sec. 340	Govern 2.1-2.3	Safety standards

APPENDIX F - SAFE HARBOR PROVISIONS

F.1 COMPLIANCE SAFE HARBORS

This appendix establishes safe harbor provisions that provide protection from enforcement actions for covered entities that demonstrate good faith compliance efforts.

F.1.1 Small Business Safe Harbor

A small business, as defined in section 110, shall be deemed to be in compliance with the requirements of this Act if it:

(1) Adopts and follows a comprehensive privacy policy that addresses the core requirements of Title V in plain language accessible to consumers;

(2) Implements reasonable security measures appropriate to the size and complexity of its operations and the sensitivity of the data it processes;

(3) Responds to consumer access, correction, and deletion requests within 45 days;

(4) Conducts a basic assessment of any AI systems it deploys to identify obvious risks or biases;

(5) Participates in an approved self-certification program, if available;

(6) Has not engaged in knowing or willful violations of this Act;

(7) Promptly remedies any violations upon becoming aware of them;

(8) Cooperates with any investigation by the Administrator or Commission.

F.1.2 Good Faith Safe Harbor

A covered entity shall not be subject to civil penalties under this Act for a violation if the covered entity demonstrates that:

(1) The violation was not knowing or willful;

(2) The covered entity had implemented a comprehensive compliance program reasonably designed to prevent violations of this Act;

(3) The compliance program included regular training for employees, periodic audits, and mechanisms for identifying and addressing compliance issues;

(4) The covered entity discovered the violation through its own compliance efforts or internal reporting mechanisms;

(5) The covered entity took prompt action to remedy the violation and prevent future occurrences;

(6) The covered entity self-reported the violation to the Administrator within 30 days of discovery;

(7) The violation did not result in substantial harm to individuals;

(8) The covered entity cooperated fully with any investigation.

F.1.3 Certification Safe Harbor

A covered entity that obtains certification from an approved certification body that its AI systems or data practices comply with the requirements of this Act shall be entitled to a rebuttable presumption of

compliance for purposes of enforcement actions, provided that:

(1) The certification was obtained from a certification body accredited by the Administrator;

(2) The certification process included independent testing and evaluation of the systems or practices at issue;

(3) The covered entity maintains the conditions on which certification was based;

(4) The covered entity promptly reports any material changes to the certification body;

(5) The certification has not been revoked or suspended.

F.2 RESEARCH AND DEVELOPMENT SAFE HARBOR

The following safe harbor provisions apply to research and development activities:

F.2.1 AI Research Exemption

The requirements of Title III, Chapters 2 through 4 shall not apply to AI systems that are:

(1) Developed and used exclusively for scientific research purposes by academic institutions, government research laboratories, or research consortia;

(2) Not deployed in production systems affecting real-world decisions;

(3) Subject to institutional review board oversight or equivalent ethical review processes;

(4) Developed using data obtained with appropriate consents or in accordance with applicable research exemptions;

(5) Not commercialized or made available for production use until compliance with applicable requirements is achieved.

F.2.2 Regulatory Sandbox

The Administrator shall establish a regulatory sandbox program that allows covered entities to test innovative AI applications under modified regulatory requirements, subject to:

(1) Participation is limited to a defined testing period not to exceed 24 months;

(2) The AI system is deployed to a limited number of users, not to exceed 10,000 individuals;

(3) Enhanced monitoring and reporting requirements are imposed;

(4) Participants agree to share learnings with the Administrator to inform future regulatory development;

(5) Clear procedures exist for exiting the sandbox and achieving full compliance;

(6) Affected individuals are informed that they are participating in a sandbox testing program and provide consent;

(7) Appropriate safeguards are in place to protect participants from harm.

APPENDIX G - DETAILED IMPLEMENTATION TIMELINE

G.1 IMPLEMENTATION MILESTONES

The following detailed timeline sets forth the implementation milestones for this Act:

Milestone	Deadline	Responsible Party
Establishment of NTGA	90 days	Secretary of Commerce
Administrator nomination	60 days	President
Administrator confirmation	120 days	Senate
Prohibition on unacceptable AI	180 days	Effective date
Priority rulemakings (NPRM)	180 days	Administrator
Priority rulemakings (Final)	365 days	Administrator
AI transparency requirements	365 days	Effective date
Large entity privacy compliance	365 days	Covered entities
Cybersecurity requirements	18 months	Effective date
High-risk AI requirements	2 years	Effective date
Small business privacy compliance	2 years	Covered entities
All rulemakings complete	2 years	Administrator
Existing AI systems compliance	3 years	Covered entities
First biennial assessment	2 years	Administrator
First comprehensive review	4 years	Administrator

G.2 PHASED COMPLIANCE SCHEDULE BY ENTITY SIZE

G.2.1 Large Covered Entities

Large covered entities, as defined in section 110, shall comply with the following schedule:

Phase 1 (6 months): Designate compliance officer; conduct initial gap assessment; establish incident reporting procedures;

Phase 2 (12 months): Implement data mapping and inventory; publish privacy policy; establish consumer rights request processes; begin AI system inventory;

Phase 3 (18 months): Complete algorithmic impact assessments for existing high-risk AI systems; implement cybersecurity requirements; establish transparency mechanisms;

Phase 4 (24 months): Achieve full compliance with all requirements; establish ongoing monitoring and compliance programs; complete conformity assessments for high-risk AI systems.

G.2.2 Medium Covered Entities

Medium covered entities (annual revenue $25M-$250M or processing data of 100,000-5,000,000 individuals) shall comply with the following schedule:

Phase 1 (12 months): Designate compliance officer; conduct initial gap assessment; publish privacy policy;

Phase 2 (18 months): Implement data mapping; establish consumer rights request processes; begin AI system inventory;

Phase 3 (24 months): Complete algorithmic impact assessments for existing high-risk AI systems; implement cybersecurity requirements;

Phase 4 (30 months): Achieve full compliance with all requirements.

G.2.3 Small Businesses

Small businesses, as defined in section 110, shall comply with the following schedule:

Phase 1 (18 months): Publish privacy policy; establish basic consumer rights request processes;

Phase 2 (24 months): Implement reasonable security measures; conduct basic AI assessment if applicable;

Phase 3 (30 months): Achieve full compliance with applicable requirements, subject to available safe harbors.

APPENDIX H - GLOSSARY OF TECHNICAL TERMS

This glossary provides additional explanation of technical terms used throughout this Act:

ACCURACY: The degree to which AI system outputs match the correct or expected results. For classification systems, accuracy is typically measured as the proportion of correct predictions out of all predictions. For regression systems, accuracy may be measured using metrics such as mean absolute error or root mean squared error.

ADVERSARIAL ATTACK: An attempt to cause an AI system to make incorrect predictions or decisions by providing carefully crafted inputs designed to exploit vulnerabilities in the system. Examples include imperceptible perturbations to images that cause misclassification.

ATTENTION MECHANISM: A component of neural network architectures that allows the model to focus on relevant parts of the input when generating outputs. Attention mechanisms are fundamental to transformer architectures used in large language models.

AUTOREGRESSIVE MODEL: A type of model that generates outputs sequentially, with each output depending on previously generated outputs. Large language models typically use autoregressive generation to produce text one token at a time.

BACKPROPAGATION: The primary algorithm used to train neural networks by computing gradients of the loss function with respect to model parameters and updating parameters to minimize loss.

BATCH NORMALIZATION: A technique used to stabilize and accelerate neural network training by normalizing layer inputs.

CHAIN-OF-THOUGHT PROMPTING: A prompting technique that encourages large language models to show intermediate reasoning steps before providing a final answer, often improving performance on complex reasoning tasks.

CLASSIFIER: An AI model that assigns inputs to discrete categories. Examples include spam detection (spam vs. not spam) and image classification (cat, dog, bird, etc.).

CONFUSION MATRIX: A table showing the performance of a classification model by comparing predicted labels to actual labels. The matrix shows true positives, true negatives, false positives, and false negatives.

CONTRASTIVE LEARNING: A self-supervised learning approach that trains models by learning to distinguish similar examples from dissimilar ones.

CONVOLUTIONAL NEURAL NETWORK (CNN): A type of neural network architecture particularly effective for image processing, using convolutional layers to detect local patterns and hierarchically build up representations.

CROSS-ENTROPY LOSS: A loss function commonly used for classification tasks that measures the difference between predicted probability distributions and actual label distributions.

DATA AUGMENTATION: Techniques for artificially expanding training datasets by creating modified versions of existing examples, such as rotated or cropped images.

DEEP LEARNING: A subset of machine learning that uses neural networks with multiple layers (deep neural networks) to learn hierarchical representations from data.

DIFFERENTIAL PRIVACY: A mathematical framework for providing provable privacy guarantees when analyzing or releasing statistical information about datasets.

DIMENSIONALITY REDUCTION: Techniques for reducing the number of features or variables in a dataset while preserving important information. Examples include principal component analysis (PCA) and t-SNE.

DISCRIMINATIVE MODEL: A model that learns to distinguish between different classes or predict labels directly from inputs, as opposed to generative models that learn the underlying data distribution.

DROPOUT: A regularization technique that randomly sets some neural network weights to zero during training to prevent overfitting.

EMBEDDING: A dense vector representation of data (such as words, images, or users) in a continuous vector space, typically learned during model training.

ENCODER-DECODER ARCHITECTURE: A neural network architecture where an encoder processes input into a latent representation and a decoder generates output from that representation. Commonly used in machine translation and summarization.

ENSEMBLE METHOD: A technique that combines predictions from multiple models to improve overall performance and robustness.

EPOCH: One complete pass through the entire training dataset during model training.

EXPLODING GRADIENTS: A problem in training deep neural networks where gradients become extremely large, causing unstable training. Various techniques exist to mitigate this issue.

F1 SCORE: A metric that combines precision and recall into a single score, calculated as the harmonic mean of precision and recall.

FALSE NEGATIVE: An error where a model incorrectly predicts a negative outcome when the actual outcome is positive.

FALSE POSITIVE: An error where a model incorrectly predicts a positive outcome when the actual outcome is negative.

FEATURE ENGINEERING: The process of creating, selecting, or transforming input features to improve model performance.

FEDERATED LEARNING: A machine learning approach where models are trained across multiple decentralized devices or servers holding local data samples, without exchanging the raw data.

FINE-TUNING: The process of taking a pre-trained model and further training it on a specific task or dataset.

FLOATING-POINT OPERATIONS (FLOPS): A measure of computing power, counting the number of arithmetic operations a computer can perform per second. Used to measure the computational requirements of AI training.

GRADIENT DESCENT: An optimization algorithm that iteratively adjusts model parameters in the direction of steepest decrease of a loss function.

GROUND TRUTH: The known correct answer or label for a data point, used to evaluate model performance.

HALLUCINATION: A phenomenon where generative AI models produce outputs that are factually incorrect, nonsensical, or not grounded in the input data.

HIDDEN LAYER: Layers in a neural network between the input and output layers that process and transform data.

HYPERPARAMETER: A parameter that controls the learning process and is set before training begins, as opposed to model parameters that are learned during training.

INFERENCE: The process of using a trained model to make predictions on new data.

IN-CONTEXT LEARNING: The ability of large language models to learn new tasks from examples provided in the prompt, without parameter updates.

KNOWLEDGE DISTILLATION: A technique for training a smaller model (student) to mimic the behavior of a larger model (teacher).

LATENT SPACE: A lower-dimensional representation of data learned by a model, capturing underlying factors of variation.

LEARNING RATE: A hyperparameter that controls how much model parameters are adjusted in response to the estimated error during training.

LOSS FUNCTION: A function that measures the difference between model predictions and actual values, guiding the training process.

MULTI-HEAD ATTENTION: An attention mechanism that runs multiple attention operations in parallel, each learning different aspects of the relationships between inputs.

NEURAL ARCHITECTURE SEARCH (NAS): Automated techniques for designing neural network architectures.

OVERFITTING: A phenomenon where a model learns to perform well on training data but fails to generalize to new data.

PARAMETER: A value in a model that is learned from data during training, such as weights in a neural network.

PERPLEXITY: A metric for evaluating language models, measuring how well the model predicts a sample of text. Lower perplexity indicates better performance.

PRECISION: The proportion of positive predictions that are actually correct. Precision = True Positives / (True Positives + False Positives).

PRE-TRAINING: Training a model on a large dataset before fine-tuning on a specific task, allowing the model to learn general representations.

PROMPT ENGINEERING: The practice of designing and optimizing input prompts to elicit desired behaviors from large language models.

RECALL: The proportion of actual positive cases that are correctly identified by the model. Recall = True Positives / (True Positives + False Negatives).

RECURRENT NEURAL NETWORK (RNN): A neural network architecture designed to process sequential data by maintaining hidden states that capture information from previous time steps.

REGULARIZATION: Techniques used to prevent overfitting by adding constraints or penalties during training.

REINFORCEMENT LEARNING FROM HUMAN FEEDBACK (RLHF): A technique for fine-tuning language models using human preferences as a reward signal.

ROC CURVE: Receiver Operating Characteristic curve, a graphical representation of a classifier's performance across different threshold settings.

SELF-SUPERVISED LEARNING: A form of unsupervised learning where the model learns representations from unlabeled data by solving pretext tasks.

SEMANTIC SIMILARITY: A measure of how closely related the meanings of two pieces of text are.

SOFTMAX: A function that converts a vector of numbers into a probability distribution.

TOKENIZATION: The process of breaking text into smaller units (tokens) for processing by a language model.

TRANSFER LEARNING: Using knowledge gained from training on one task to improve performance on a related task.

TRANSFORMER: A neural network architecture based on self-attention mechanisms, forming the basis for most large language models.

UNDERFITTING: A phenomenon where a model is too simple to capture the underlying patterns in the data.

VANISHING GRADIENTS: A problem in training deep neural networks where gradients become extremely small, slowing or preventing learning in early layers.

WORD EMBEDDING: A learned representation of text where words with similar meanings have similar vector representations.

ZERO-SHOT LEARNING: The ability of a model to perform tasks it was not explicitly trained on, without any task-specific examples.

APPENDIX I - MODEL FORMS AND NOTICES

I.1 MODEL PRIVACY NOTICE

The following model privacy notice may be used by covered entities to satisfy the privacy policy requirements of section 502(e). Covered entities may adapt this notice to reflect their specific practices:

[COMPANY NAME] PRIVACY NOTICE

Last Updated: [DATE]

What Information We Collect

We collect information you provide directly, such as when you create an account, make a purchase, or contact us. We also collect information automatically through cookies and similar technologies, including your IP address, browser type, and browsing activity.

How We Use Your Information

We use your information to provide and improve our services, process transactions, communicate with you, and for security and fraud prevention. We may also use your information for marketing purposes with your consent.

How We Share Your Information

We may share your information with service providers who help us operate our business, with your consent, or as required by law. We do not sell your personal information.

Your Privacy Rights

Depending on where you live, you may have rights to access, correct, delete, or port your personal information. You may also have the right to opt out of certain uses of your information. To exercise these rights, contact us at [CONTACT INFORMATION].

Data Retention

We retain your information for as long as necessary to provide our services and fulfill the purposes described in this notice, unless a longer retention period is required by law.

Security

We implement reasonable security measures to protect your information. However, no system is completely secure.

Children's Privacy

Our services are not directed to children under 13. We do not knowingly collect personal information from children under 13.

Changes to This Notice

We may update this notice from time to time. We will notify you of material changes by posting the updated notice on our website.

Contact Us

If you have questions about this notice or our privacy practices, contact us at [CONTACT INFORMATION].

I.2 MODEL AI DISCLOSURE NOTICE

The following model notice may be used to satisfy the AI disclosure requirements of section 320:

AI SYSTEM DISCLOSURE

[COMPANY NAME] uses artificial intelligence in [DESCRIPTION OF USE, e.g., 'our customer service chat,' 'our hiring process,' 'our content recommendations']. This notice explains how AI is used and your rights.

How AI Is Used

We use AI to [specific description of how AI assists in the process]. The AI system [makes recommendations/assists human decision-makers/makes automated decisions] regarding [subject matter].

Human Oversight

[Description of human review process, e.g., 'All AI recommendations are reviewed by a human before final decisions are made' or 'The AI makes initial screening decisions, which are reviewed by humans upon request.']

Your Rights

You have the right to: (1) know when AI is being used in decisions affecting you; (2) receive an explanation of how the AI reached its recommendation or decision; (3) request human review of AI-assisted decisions; (4) contest decisions you believe are incorrect.

How to Exercise Your Rights

To request more information about AI-assisted decisions, obtain an explanation, or request human review, contact us at [CONTACT INFORMATION]. We will respond to your request within [TIMEFRAME].

More Information

For more information about our AI practices, please see [LINK TO DETAILED DOCUMENTATION].

I.3 MODEL CONSUMER RIGHTS REQUEST FORM

The following model form may be used by consumers to submit privacy rights requests:

PRIVACY RIGHTS REQUEST FORM

Full Name: _____

Email Address: _____

Phone Number (optional): _____

Mailing Address (optional): _____

I am submitting this request as (check one):

[ ] The consumer whose personal information is the subject of this request

[ ] An authorized agent acting on behalf of the consumer

I am requesting (check all that apply):

[ ] Access to my personal information

[ ] Correction of inaccurate personal information

[ ] Deletion of my personal information

[ ] A copy of my personal information in a portable format

[ ] To opt out of the sale or sharing of my personal information

[ ] To opt out of targeted advertising

[ ] To opt out of profiling for automated decisions

[ ] Information about AI systems used to make decisions about me

[ ] Human review of an AI-assisted decision

Please describe your request in detail:

_____

_____

_____

For correction requests, please specify what information is inaccurate and provide the correct information:

_____

_____

Verification Information (to help us verify your identity):

Account username or ID (if applicable): _____

Recent transaction or interaction (if applicable): _____

Signature: _____ Date: _____

Passed the House of Representatives [DATE]

_____

Clerk of the House of Representatives

Passed the Senate [DATE]

_____

Secretary of the Senate

*** * * END OF DOCUMENT * * ***