relating to ''Circumvention of Lawful Pathways''.

S.J. RES. 49

At the request of Mr. CASSIDY, the names of the Senator from Florida (Mr. SCOTT), the Senator from Arkansas (Mr. COTTON), the Senator from Wyoming (Ms. LUMMIS), the Senator from Iowa (Ms. ERNST), the Senator from Tennessee (Mrs. BLACKBURN), and the Senator from Utah (Mr. ROMNEY) were added as cosponsors of S.J. Res. 49, a joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the National Labor Relations Board relating to a ''Standard for Determining Joint Employer Status''.

S. RES. 20

At the request of Mr. CARDIN, the name of the Senator from Massachusetts (Ms. WARREN) was added as a cosponsor of S. Res. 20, a resolution condemning the coup that took place on February 1, 2021, in Burma and the Burmese military's detention of civilian leaders, calling for an immediate and unconditional release of all those detained, promoting accountability and justice for those killed by the Burmese military, and calling for those elected to serve in parliament to resume their duties without impediment, and for other purposes.

S. RES. 333

At the request of Mr. DURBIN, the name of the Senator from Maryland (Mr. VAN HOLLEN) was added as a cosponsor of S. Res. 333, a resolution designating 2024 as the Year of Democracy as a time to reflect on the contributions of the system of Government of the United States to a more free and stable world.

S. RES. 385

At the request of Mr. CARDIN, the name of the Senator from Delaware (Mr. COONS) was added as a cosponsor of S. Res. 385, a resolution calling for the immediate release of Evan Gershkovich, a United States citizen and journalist, who was wrongfully detained by the Government of the Russian Federation in March 2023.

S. RES. 408

At the request of Ms. ROSEN, the name of the Senator from Oregon (Mr. MERKLEY) was added as a cosponsor of S. Res. 408, a resolution condemning Hamas for its premeditated, coordinated, and brutal terrorist attacks on Israel and demanding that Hamas immediately release all hostages and return them to safety, and for other purposes.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. THUNE (for himself, Ms. KLOBUCHAR, Mr. WICKER, Mr. HICKENLOOPER, Mr. LUJÁN, and Mrs. CAPITO):

S. 3312. A bill to provide a framework for artificial intelligence innovation and accountability, and for other purposes; to the Committee on Commerce, Science, and Transportation.

Mr. THUNE. Madam President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 3312

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Artificial Intelligence Research, Innovation, and Accountability Act of 2023''.

SEC. 2. TABLE OF CONTENTS.

The table of contents for this Act is as follows:

Sec. 1. Short title.
Sec. 2. Table of contents.

TITLE I—ARTIFICIAL INTELLIGENCE RESEARCH AND INNOVATION

Sec. 101. Open data policy amendments.
Sec. 102. Online content authenticity and provenance standards research and development.
Sec. 103. Standards for detection of emergent and anomalous behavior and AI-generated media.
Sec. 104. Comptroller General study on barriers and best practices to usage of AI in government.

TITLE II—ARTIFICIAL INTELLIGENCE ACCOUNTABILITY

Sec. 201. Definitions.
Sec. 202. Generative artificial intelligence transparency.
Sec. 203. Transparency reports for high-impact artificial intelligence systems.
Sec. 204. Recommendations to Federal agencies for risk management of high-impact artificial intelligence systems.
Sec. 205. Office of management and budget oversight of recommendations to agencies.
Sec. 206. Risk management assessment for critical-impact artificial intelligence systems.
Sec. 207. Certification of critical-impact artificial intelligence systems.
Sec. 208. Enforcement.
Sec. 209. Artificial intelligence consumer education.

TITLE I—ARTIFICIAL INTELLIGENCE RESEARCH AND INNOVATION

SEC. 101. OPEN DATA POLICY AMENDMENTS.

Section 3502 of title 44, United States Code, is amended—

(1) in paragraph (22)—

(A) by inserting ''or data model'' after ''a data asset''; and

(B) by striking ''and'' at the end;

(2) in paragraph (23), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

''(24) the term 'data model' means a mathematical, economic, or statistical representation of a system or process used to assist in making calculations and predictions, including through the use of algorithms, computer programs, or artificial intelligence systems; and

''(25) the term 'artificial intelligence system' means an engineered system that—

''(A) generates outputs, such as content, predictions, recommendations, or decisions for a given set of objectives; and

''(B) is designed to operate with varying levels of adaptability and autonomy using machine and human-based inputs.''.

SEC. 102. ONLINE CONTENT AUTHENTICITY AND PROVENANCE STANDARDS RESEARCH AND DEVELOPMENT.

(a) RESEARCH.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this Act, the Under Secretary of Commerce for Standards and Technology shall carry out research to facilitate the development and standardization of means to provide authenticity and provenance information for content generated by human authors and artificial intelligence systems.

(2) ELEMENTS.—The research carried out pursuant to paragraph (1) shall cover the following:

(A) Secure and binding methods for human authors of content to append statements of provenance through the use of unique credentials, watermarking, or other data or metadata-based approaches.

(B) Methods for the verification of statements of content provenance to ensure authenticity such as watermarking or classifiers, which are trained models that distinguish artificial intelligence-generated media.

(C) Methods for displaying clear and conspicuous statements of content provenance to the end user.

(D) Technologies or applications needed to facilitate the creation and verification of content provenance information.

(E) Mechanisms to ensure that any technologies and methods developed under this section are minimally burdensome on content producers.

(F) Such other related processes, technologies, or applications as the Under Secretary considers appropriate.

(G) Use of provenance technology to enable attribution for content creators.

(3) IMPLEMENTATION.—The Under Secretary shall carry out the research required by paragraph (1) as part of the research directives pursuant to section 22A(b)(1) of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1(b)(1)).

(b) DEVELOPMENT OF STANDARDS.—

(1) IN GENERAL.—For methodologies and applications related to content provenance and authenticity deemed by the Under Secretary to be at a readiness level sufficient for standardization, the Under Secretary shall provide technical review and assistance to such other Federal agencies and nongovernmental standards organizations as the Under Secretary considers appropriate.

(2) CONSIDERATIONS.—In providing any technical review and assistance related to the development of content provenance and authenticity standards under this subsection, the Under Secretary may—

(A) consider whether a proposed standard is reasonable, practicable, and appropriate for the particular type of media and media environment for which the standard is proposed;

(B) consult with relevant stakeholders; and

(C) review industry standards issued by nongovernmental standards organizations.

(c) PILOT PROGRAM.—

(1) IN GENERAL.—The Under Secretary shall carry out a pilot program to assess the feasibility and advisability of using available technologies and creating open standards to facilitate the creation and verification of content governance information for digital content.

(2) LOCATIONS.—The pilot program required by paragraph (1) shall be carried out at not more than 2 Federal agencies the Under Secretary shall select for purposes of the pilot program required by paragraph (1).

(3) REQUIREMENTS.—In carrying out the pilot program required by paragraph (1), the Under Secretary shall—

(A) apply and evaluate methods for authenticating the origin of and modifications to government-produced digital content using technology and open standards described in paragraph (1); and

(B) make available to the public digital content embedded with provenance or other authentication provided by the heads of the Federal agencies selected pursuant to paragraph (2) for the purposes of the pilot program.

(4) Briefing required.—Not later than 1 year after the date of the enactment of this Act, and annually thereafter until the date described in paragraph (5), the Under Secretary shall brief the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives on the findings of the Under Secretary with respect to the pilot program carried out under this subsection.

(5) Termination.—The pilot program shall terminate on the date that is 10 years after the date of the enactment of this Act.

(d) Report to Congress.—Not later than 1 year after the date of the enactment of this Act, the Under Secretary shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report outlining the progress of standardization initiatives relating to requirements under this section, as well as recommendations for legislative or administrative action to encourage or require the widespread adoption of such initiatives in the United States.

SEC. 103. STANDARDS FOR DETECTION OF EMERGENT AND ANOMALOUS BEHAVIOR AND AI-GENERATED MEDIA.

Section 22A(b)(1) of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1(b)(1)) is amended—

(1) by redesignating subparagraph (I) as subparagraph (K);

(2) in subparagraph (H), by striking ''; and'' and inserting a semicolon; and

(3) by inserting after subparagraph (H) the following:

''(I) best practices for detecting outputs generated by artificial intelligence systems, including content such as text, audio, images, and videos;

''(J) methods to detect and understand anomalous behavior of artificial intelligence systems and safeguards to mitigate potentially adversarial or compromising anomalous behavior; and''.

SEC. 104. COMPTROLLER GENERAL STUDY ON BARRIERS AND BEST PRACTICES TO USAGE OF AI IN GOVERNMENT.

(a) In General.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall—

(1) conduct a review of statutory, regulatory, and other policy barriers to the use of artificial intelligence systems to improve the functionality of the Federal Government; and

(2) identify best practices for the adoption and use of artificial intelligence systems by the Federal Government, including—

(A) ensuring that an artificial intelligence system is proportional to the need of the Federal Government;

(B) restrictions on access to and use of an artificial intelligence system based on the capabilities and risks of the artificial intelligence system; and

(C) safety measures that ensure that an artificial intelligence system is appropriately limited to necessary data and compartmentalized from other assets of the Federal Government.

(b) Report.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives a report that—

(1) summarizes the results of the review conducted under subsection (a)(1) and the best practices identified under subsection (a)(2), including recommendations, as the Comptroller General of the United States considers appropriate;

(2) describes any laws, regulations, guidance documents, or other policies that may prevent the adoption of artificial intelligence systems by the Federal Government to improve certain functions of the Federal Government, including—

(A) data analysis and processing;

(B) paperwork reduction;

(C) contracting and procurement practices; and

(D) other Federal Government services; and

(3) includes, as the Comptroller General of the United States considers appropriate, recommendations to modify or eliminate barriers to the use of artificial intelligence systems by the Federal Government.

TITLE II—ARTIFICIAL INTELLIGENCE ACCOUNTABILITY

SEC. 201. DEFINITIONS.

In this title:

(1) Appropriate congressional committees.—The term ''appropriate congressional committees'' means—

(A) the Committee on Energy and Natural Resources and the Committee on Commerce, Science, and Transportation of the Senate;

(B) the Committee on Energy and Commerce of the House of Representatives; and

(C) each congressional committee with jurisdiction over an applicable covered agency.

(2) Artificial intelligence system.—The term ''artificial intelligence system'' means an engineered system that—

(A) generates outputs, such as content, predictions, recommendations, or decisions for a given set of human-defined objectives; and

(B) is designed to operate with varying levels of adaptability and autonomy using machine and human-based inputs.

(3) Covered agency.—the term ''covered agency'' means an agency for which the Under Secretary develops an NIST recommendation.

(4) Covered internet platform.—

(A) In general.—The term ''covered internet platform''—

(i) means any public-facing website, consumer-facing internet application, or mobile application available to consumers in the United States; and

(ii) includes a social network site, video sharing service, search engine, and content aggregation service.

(B) Exclusions.—The term ''covered internet platform'' does not include a platform that—

(i) is wholly owned, controlled, and operated by a person that—

(I) during the most recent 180-day period, did not employ more than 500 employees;

(II) during the most recent 3-year period, averaged less than $50,000,000 in annual gross receipts; and

(III) on an annual basis, collects or processes the personal data of less than 1,000,000 individuals; or

(ii) is operated for the sole purpose of conducting research that is not directly or indirectly made for profit.

(5) Critical-impact AI organization.—The term ''critical-impact AI organization'' means a non-government organization that serves as the deployer of a critical-impact artificial intelligence system.

(6) Critical-impact artificial intelligence system.—The term ''critical-impact artificial intelligence system'' means an artificial intelligence system that—

(A) is deployed for a purpose other than solely for use by the Department of Defense or an intelligence agency (as defined in section 3094(e) of the National Security Act of 1947 (50 U.S.C. 3094(3)) ; and

(B) is used or intended to be used—

(i) to make decisions that have a legal or similarly significant effect on—

(I) the real-time or ex post facto collection of biometric data of natural persons by biometric identification systems without their consent;

(II) the direct management and operation of critical infrastructure (as defined in section 1016(e) of the USA PATRIOT Act (42 U.S.C. 5195c(e)) and space-based infrastructure; or

(III) criminal justice (as defined in section 901 of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (34 U.S.C. 10251)); and

(ii) in a manner that poses a significant risk to rights afforded under the Constitution of the United States or safety.

(7) Deployer.—The term ''deployer''—

(A) means an entity that uses or operates an artificial intelligence system for internal use or for use by third parties; and

(B) does not include an entity that is solely an end user of a system.

(8) Developer.—The term ''developer'' means an entity that—

(A) designs, codes, produces, or owns an artificial intelligence system for internal use or for use by a third party as a baseline model; and

(B) does not act as a deployer of the artificial intelligence system described in subparagraph (A).

(9) Generative artificial intelligence system.—The term ''generative artificial intelligence system'' means an artificial intelligence system that generates novel data or content in a written, audio, or visual format.

(10) High-impact artificial intelligence system.—The term ''high-impact artificial intelligence system'' means an artificial intelligence system—

(A) deployed for a purpose other than solely for use by the Department of Defense or an intelligence agency (as defined in section 3094(e) of the National Security Act of 1947 (50 U.S.C. 3094(3)); and

(B) that is specifically developed with the intended purpose of making decisions that have a legal or similarly significant effect on the access of an individual to housing, employment, credit, education, healthcare, or insurance in a manner that poses a significant risk to rights afforded under the Constitution of the United States or safety.

(11) NIST recommendation.—The term ''NIST recommendation'' means a sector-specific recommendation developed under section 22B(b)(1) of the National Institute of Standards and Technology Act, as added by section 204 of this Act.

(12) Secretary.—The term ''Secretary'' means the Secretary of Commerce.

(13) Significant risk.—The term ''significant risk'' means a combination of severe, high-intensity, high-probability, and long-duration risk of harm to individuals.

(14) TEVV.—The term ''TEVV'' means the testing, evaluation, validation, and verification of any artificial intelligence system that includes—

(A) open, transparent, testable, and verifiable specifications that characterize realistic operational performance, such as precision and accuracy for relevant tasks;

(B) testing methodologies and metrics that enable the evaluation of system trustworthiness, including robustness and resilience;

(C) data quality standards for training and testing datasets;

(D) requirements for system validation and integration into production environments, automated testing, and compliance with existing legal and regulatory specifications;

(E) methods and tools for—

(i) the monitoring of system behavior;

(ii) the tracking of incidents or errors reported and their management; and

(iii) the detection of emergent properties and related impacts; and

(F) and processes for redress and response.

(15) UNDER SECRETARY.—The term ''Under Secretary'' means the Director of the National Institute of Standards and Technology.

SEC. 202. GENERATIVE ARTIFICIAL INTELLIGENCE TRANSPARENCY.

(a) PROHIBITION.—

(1) IN GENERAL.—Subject to paragraph (2), it shall be unlawful for a person to operate a covered internet platform that uses a generative artificial intelligence system.

(2) DISCLOSURE OF USE OF GENERATIVE ARTIFICIAL INTELLIGENCE SYSTEMS.—

(A) IN GENERAL.—A person may operate a covered internet platform that uses a generative artificial intelligence system if the person provides notice to each user of the covered internet platform that the covered internet platform uses a generative artificial intelligence system to generate content the user sees.

(B) REQUIREMENTS.—A person providing the notice described in subparagraph (A) to a user—

(i) subject to clause (ii), shall provide the notice in a clear and conspicuous manner on the covered internet platform before the user interacts with content produced by a generative artificial intelligence system; and

(ii) may provide an option for the user to choose to see the notice described in clause (i) only upon the first interaction of the user with content produced by a generative artificial intelligence system.

(b) ENFORCEMENT ACTION.—Upon learning that a covered internet platform does not comply with the requirements under this section, the Secretary—

(1) shall immediately—

(A) notify the covered internet platform of the finding; and

(B) order the covered internet platform to take remedial action to address the noncompliance of the generative artificial intelligence system operated by the covered internet platform; and

(2) may, as determined appropriate or necessary by the Secretary, take enforcement action under section 208 if the covered internet platform does not take sufficient action to remedy the noncompliance within 15 days of the notification under paragraph (1)(A).

(c) EFFECTIVE DATE.—This section shall take effect on the date that is 180 days after the date of enactment of this Act.

SEC. 203. TRANSPARENCY REPORTS FOR HIGH-IMPACT ARTIFICIAL INTELLIGENCE SYSTEMS.

(a) TRANSPARENCY REPORTING.—

(1) IN GENERAL.—Each deployer of a high-impact artificial intelligence system shall—

(A) before deploying the high-impact artificial intelligence system, and annually thereafter, submit to the Secretary a report describing the design and safety plans for the artificial intelligence system; and

(B) submit to the Secretary an updated report on the high-impact artificial intelligence system if the deployer makes a material change to—

(i) the purpose for which the high-impact artificial intelligence system is used; or

(ii) the type of data the high-impact artificial intelligence system processes or uses for training purposes.

(2) CONTENTS.—Each transparency report submitted under paragraph (1) shall include, with respect to the high-impact artificial intelligence system—

(A) the purpose;

(B) the intended use cases;

(C) deployment context;

(D) benefits;

(E) a description of data that the high-impact artificial intelligence system, once deployed, processes as inputs;

(F) if available—

(i) a list of data categories and formats the deployer used to retrain or continue training the high-impact artificial intelligence system;

(ii) metrics for evaluating the high-impact artificial intelligence system performance and known limitations; and

(iii) transparency measures, including information identifying to individuals when a high-impact artificial intelligence system is in use;

(G) processes and testing performed before each deployment to ensure the high-impact artificial intelligence system is safe, reliable, and effective;

(H) if applicable, an identification of any third-party artificial intelligence systems or datasets the deployer relies on to train or operate the high-impact artificial intelligence system; and

(I) post-deployment monitoring and user safeguards, including a description of the oversight process in place to address issues as issues arise.

(b) DEVELOPER OBLIGATIONS.—The developer of a high-impact artificial intelligence system shall be subject to the same obligations as a developer of a critical impact artificial intelligence system under section 206(c).

(c) CONSIDERATIONS.—In carrying out subsection (a) and (b), a deployer or developer of a high-impact artificial intelligence system shall consider the best practices outlined in the most recent version of the risk management framework developed pursuant to section 22A(c) of the National Institute of Standards and Technology Act (15 U.S.C. 278h–1(c)).

(d) NONCOMPLIANCE AND ENFORCEMENT ACTION.—Upon learning that a deployer of a high-impact artificial intelligence system is not in compliance with the requirements under this section with respect to a high-impact artificial intelligence system, the Secretary—

(1) shall immediately—

(A) notify the deployer of the finding; and

(B) order the deployer to immediately submit to the Secretary the report required under subsection (a)(1); and

(2) if the deployer fails to submit the report by the date that is 15 days after the date of the notification under paragraph (1)(A), may take enforcement action under section 208.

(e) AVOIDANCE OF DUPLICATION.—

(1) IN GENERAL.—Pursuant to the deconfliction of duplicative requirements under paragraph (2), the Secretary shall ensure that the requirements under this section are not unnecessarily burdensome or duplicative of requirements made or oversight conducted by a covered agency regarding the non-Federal use of high-impact artificial intelligence systems.

(2) DECONFLICTION OF DUPLICATIVE REQUIREMENTS.—Not later than 90 days after the date of the enactment of this Act, and annually thereafter, the Secretary, in coordination with the head of any relevant covered agency, shall complete the deconfliction of duplicative requirements relating to the submission of a transparency report for a high-impact artificial intelligence system under this section.

(f) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to require a deployer of a high-impact artificial intelligence system to disclose any information, including data or algorithms—

(1) relating to a trade secret or other protected intellectual property right;

(2) that is confidential business information; or

(3) that is privileged.

SEC. 204. RECOMMENDATIONS TO FEDERAL AGENCIES FOR RISK MANAGEMENT OF HIGH-IMPACT ARTIFICIAL INTELLIGENCE SYSTEMS.

The National Institute of Standards and Technology Act (15 U.S.C. 278h–1) is amended by inserting after section 22A the following:

''SEC. 22B. RECOMMENDATIONS TO FEDERAL AGENCIES FOR SECTOR-SPECIFIC OVERSIGHT OF ARTIFICIAL INTELLIGENCE.

''(a) DEFINITION OF HIGH-IMPACT ARTIFICIAL INTELLIGENCE SYSTEM.—In this section, the term 'high-impact artificial intelligence system' means an artificial intelligence system—

''(1) deployed for purposes other than those solely for use by the Department of Defense or an element of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)); and

''(2) that is specifically developed with the intended purpose of making decisions that have a legal or similarly significant effect on the access of an individual to housing, employment, credit, education, health care, or insurance in a manner that poses a significant risk to rights afforded under the Constitution of the United States or to safety.

''(b) SECTOR-SPECIFIC RECOMMENDATIONS.—Not later than 1 year after the date of the enactment of the Artificial Intelligence Research, Innovation, and Accountability Act of 2023, the Director shall—

''(1) develop sector-specific recommendations for individual Federal agencies to conduct oversight of the non-Federal, and, as appropriate, Federal use of high-impact artificial intelligence systems to improve the safe and responsible use of such systems; and

''(2) not less frequently than biennially, update the sector-specific recommendations to account for changes in technological capabilities or artificial intelligence use cases.

''(c) REQUIREMENTS.—In developing recommendations under subsection (b), the Director shall use the voluntary risk management framework required by section 22A(c) to identify and provide recommendations to a Federal agency—

''(1) to establish regulations, standards, guidelines, best practices, methodologies, procedures, or processes to facilitate oversight of non-Federal use of high-impact artificial intelligence systems;

''(2) to mitigate risks from such high-impact artificial intelligence systems.

''(d) RECOMMENDATIONS.—In developing recommendations under subsection (b), the Director may include the following:

''(1) Key design choices made during high-impact artificial intelligence model development, including rationale and assumptions made.

''(2) Intended use and users, other possible use cases, including any anticipated undesirable or potentially harmful use cases, and what good faith efforts model developers can take to mitigate the use of the system in harmful ways.

''(3) Methods for evaluating the safety of high-impact artificial intelligence systems and approaches for responsible use.

''(4) Sector-specific differences in what constitutes acceptable high-impact artificial intelligence model functionality and trustworthiness, metrics used to determine high-impact artificial intelligence model performance, and any test results reflecting application of these metrics to evaluate high-impact artificial intelligence model performance across different sectors.

''(5) Recommendations to support iterative development of subsequent recommendations under subsection (b).

''(e) Consultation.—In developing recommendations under subsection (b), the Director shall, as the Director considers applicable and practicable, consult with relevant covered agencies and stakeholders representing perspectives from civil society, academia, technologists, engineers, and creators.''.

SEC. 205. OFFICE OF MANAGEMENT AND BUDGET OVERSIGHT OF RECOMMENDATIONS TO AGENCIES.

(a) Recommendations.—

(1) In general.—Not later than 1 year after the date of enactment of this Act, the Under Secretary shall submit to the Director, the head each covered agency, and the appropriate congressional committees each NIST recommendation.

(2) Agency responses to recommendations.—Not later than 90 days after the date on which the Under Secretary submits a NIST recommendation to the head of a covered agency under paragraph (1), the head of the covered agency shall transmit to the Director a formal written response to the NIST recommendation that—

(A) indicates whether the head of the covered agency intends to—

(i) carry out procedures to adopt the complete NIST recommendation;

(ii) carry out procedures to adopt a part of the NIST recommendation; or

(iii) refuse to carry out procedures to adopt the NIST recommendation; and

(B) includes—

(i) with respect to a formal written response described in clause (i) or (ii) of subparagraph (A), a copy of a proposed timetable for completing the procedures described in that clause;

(ii) with respect to a formal written response described in subparagraph (A)(ii), the reasons for the refusal to carry out procedures with respect to the remainder of the NIST recommendation described in that subparagraph; and

(iii) with respect to a formal written response described in subparagraph (A)(iii), the reasons for the refusal to carry out procedures.

(b) Public Availability.—The Director shall make a copy of each NIST recommendation and each written formal response of a covered agency required under subsection (a)(2) available to the public at reasonable cost.

(c) Reporting Requirements.—

(1) Annual secretarial regulatory status reports.—

(A) In general.—On the first February 1 occurring after the date of enactment of this Act, and annually thereafter until the date described in subparagraph (B), the head of each covered agency shall submit to the Director a report containing the regulatory status of each NIST recommendation.

(B) Continued reporting.—The date described in this subparagraph is the date on which the head of a covered agency—

(i) takes final regulatory action with respect to a NIST recommendation; and

(ii) determines and states in a report required under subparagraph (A) that no regulatory action should be taken with respect to a NIST recommendation.

(2) Compliance report to congress.—On April 1 of each year, the Director shall—

(A) review the reports received under paragraph (1)(A); and

(B) transmit comments on the reports to the heads of covered agencies and the appropriate congressional committees.

(3) Failure to report.—If, on March 1 of each year, the Director has not received a report required under paragraph (1)(A) from the head of a covered agency, the Director shall notify the appropriate congressional committees of the failure.

(d) Technical Assistance in Carrying Out Recommendations.—The Under Secretary shall provide assistance to the heads of covered agencies relating to the implementation of the NIST recommendations the heads of covered agencies intend to carry out.

(e) Regulation Review and Improvement.—The Administrator of the Office of Information and Regulatory Affairs of the Office of Management and Budget, in consultation with the Under Secretary, shall develop and periodically revise performance indicators and measures for sector-specific regulation of artificial intelligence.

SEC. 206. RISK MANAGEMENT ASSESSMENT FOR CRITICAL-IMPACT ARTIFICIAL INTELLIGENCE SYSTEMS.

(a) Requirement.—

(1) In general.—Each critical-impact AI organization shall perform a risk management assessment in accordance with this section.

(2) Assessment.—Each critical-impact AI organization shall—

(A) not later than 30 days before the date on which a critical-impact artificial intelligence system is made publicly available by the critical-impact AI organization, perform a risk management assessment; and

(B) not less frequently than biennially during the period beginning on the date of enactment of this Act and ending on the date on which the applicable critical-impact artificial intelligence system is no longer being made publicly available by the critical-impact AI organization, as applicable, conduct an updated risk management assessment that—

(i) may find that no significant changes were made to the critical-impact artificial intelligence system; and

(ii) provides, to the extent practicable, aggregate results of any significant deviation from expected performance detailed in the assessment performed under subparagraph (A) or the most recent assessment performed under this subparagraph.

(3) Review.—

(A) In general.—Not later than 90 days after the date of completion of a risk management assessment by a critical-impact AI organization under this section, the critical-impact AI organization shall submit to the Secretary a report—

(i) outlining the assessment performed under this section; and

(ii) that is in a consistent format, as determined by the Secretary.

(B) Additional information.—Subject to subsection (d), the Secretary may request that a critical-impact AI organization submit to the Secretary any related additional or clarifying information with respect to a risk management assessment performed under this section.

(4) Limitation.— The Secretary may not prohibit a critical-impact AI organization from making a critical-impact artificial intelligence system available to the public based on the review by the Secretary of a report submitted under paragraph (3)(A) or additional or clarifying information submitted under paragraph (3)(B).

(b) Assessment Subject Areas.—Each assessment performed by a critical-impact AI organization under subsection (a) shall describe the means by which the critical-impact AI organization is addressing, through a documented TEVV process, the following categories:

(1) Policies, processes, procedures, and practices across the organization relating to transparent and effective mapping, measuring, and managing of artificial intelligence risks, including—

(A) how the organization understands, manages, and documents legal and regulatory requirements involving artificial intelligence;

(B) how the organization integrates characteristics of trustworthy artificial intelligence, which include valid, reliable, safe, secure, resilient, accountable, transparent, globally and locally explainable, interpretable, privacy-enhanced, and fair with harmful bias managed, into organizational policies, processes, procedures, and practices;

(C) a methodology to determine the needed level of risk management activities based on the organization's risk tolerance; and

(D) how the organization establishes risk management processes and outcomes through transparent policies, procedures, and other controls based on organizational risk priorities.

(2) The structure, context, and capabilities of the critical-impact artificial intelligence system or critical-impact foundation model, including—

(A) how the context was established and understood;

(B) capabilities, targeted uses, goals, and expected costs and benefits; and

(C) how risks and benefits are mapped for each system component.

(3) A description of how the organization employs quantitative, qualitative, or mixed-method tools, techniques, and methodologies to analyze, assess, benchmark, and monitor artificial intelligence risk, including—

(A) identification of appropriate methods and metrics;

(B) how artificial intelligence systems are evaluated for trustworthy characteristics;

(C) mechanisms for tracking artificial intelligence system risks over time; and

(D) processes for gathering and assessing feedback relating to the efficacy of measurement.

(4) A description of allocation of risk resources to map and measure risks on a regular basis as described in paragraph (1), including—

(A) how artificial intelligence risks based on assessments and other analytical outputs described in paragraphs (2) and (3) are prioritized, responded to, and managed;

(B) how strategies to maximize artificial intelligence benefits and minimize negative impacts were planned, prepared, implemented, documented, and informed by input from relevant artificial intelligence deployers;

(C) management of artificial intelligence system risks and benefits; and

(D) regular monitoring of risk treatments, including response and recovery, and communication plans for the identified and measured artificial intelligence risks, as applicable.

(c) Developer Obligations.—The developer of a critical-impact artificial intelligence system that agrees through a contract or license to provide technology or services to a deployer of the critical-impact artificial intelligence system shall provide to the deployer of the critical-impact artificial intelligence system the information reasonably necessary for the deployer to comply with the requirements under subsection (a), including—

(1) an overview of the data used in training the baseline artificial intelligence system provided by the developer, including—

(A) data size;

(B) data sources;

(C) copyrighted data; and

(D) personal identifiable information;

(2) documentation outlining the structure and context of the baseline artificial intelligence system of the developer, including—

(A) input modality;

(B) output modality;

(C) model size; and

(D) model architecture;

(3) known capabilities, limitations, and risks of the baseline artificial intelligence system of the developer at the time of the development of the artificial intelligence system; and

(4) documentation for downstream use, including—

(A) a statement of intended purpose;

(B) guidelines for the intended use of the artificial intelligence system, including a list of permitted, restricted, and prohibited uses and users; and

(C) a statement of the potential for deviation from the intended purpose of the baseline artificial intelligence system.

(d) Termination of Obligation to Disclose Information.—

(1) In general.—The obligation of a critical-impact AI organization to provide information, upon request of the Secretary, relating to a specific assessment category under subsection (b) shall end on the date of issuance of a relevant standard applicable to the same category of a critical -impact artificial intelligence system by—

(A) the Secretary under section 207(c) with respect to a critical-impact artificial intelligence system;

(B) another department or agency of the Federal Government, as determined applicable by the Secretary; or

(C) a non-governmental standards organization, as determined appropriate by the Secretary.

(2) Effect of new standard.—In adopting any standard applicable to critical-impact artificial intelligence systems under section 207(c), the Secretary shall—

(A) identify the category under subsection (b) to which the standard relates, if any; and

(B) specify the information that is no longer required to be included in a report required under subsection (a) as a result of the new standard.

(e) Rule of Construction.—Nothing in this section shall be construed to require a critical-impact AI organization, or permit the Secretary, to disclose any information, including data or algorithms—

(1) relating to a trade secret or other protected intellectual property right;

(2) that is confidential business information; or

(3) that is privileged.

SEC. 207. CERTIFICATION OF CRITICAL-IMPACT ARTIFICIAL INTELLIGENCE SYSTEMS.

(a) Establishment of Artificial Intelligence Certification Advisory Committee.—

(1) In general.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish an advisory committee to provide advice and recommendations on TEVV standards and the certification of critical-impact artificial intelligence systems.

(2) Duties.—The advisory committee established under this section shall advise the Secretary on matters relating to the testing and certification of critical-impact artificial intelligence systems, including by—

(A) providing recommendations to the Secretary on proposed TEVV standards to ensure such standards—

(i) maximize alignment and interoperability with standards issued by nongovernmental standards organizations and international standards bodies;

(ii) are performance-based and impact-based; and

(iii) are applicable or necessary to facilitate the deployment of critical-impact artificial intelligence systems in a transparent, secure, and safe manner;

(B) reviewing prospective TEVV standards submitted by the Secretary to ensure such standards align with recommendations under subparagraph (A);

(C) upon completion of the review under subparagraph (B), providing consensus recommendations to the Secretary on—

(i) whether a TEVV standard should be issued, modified, revoked, or added; and

(ii) if such a standard should be issued, how best to align the standard with the considerations described in subsection (c)(2) and recommendations described in subparagraph (A); and

(D) reviewing and providing advice and recommendations on the plan and subsequent updates to the plan submitted under subsection (b).

(3) Composition.—The advisory committee established under this subsection shall be composed of not more than 15 members with a balanced composition of representatives of the private sector, institutions of higher education, and non-profit organizations, including—

(A) representatives of—

(i) institutions of higher education;

(ii) companies developing or operating artificial intelligence systems;

(iii) consumers or consumer advocacy groups; and

(iv) enabling technology companies; and

(B) any other members the Secretary considers to be appropriate.

(b) Artificial Intelligence Certification Plan.—

(1) In general.—Not later than 1 year after the date of enactment of this Act, the Secretary shall establish a 3-year implementation plan for the certification of critical-impact artificial intelligence systems.

(2) Periodic update.—The Secretary shall periodically update the plan established under paragraph (1).

(3) Contents.—The plan established under paragraph (1) shall include—

(A) a methodology for gathering and using relevant, objective, and available information relating to TEVV;

(B) a process for considering whether prescribing certain TEVV standards under subsection (c) for critical-impact artificial intelligence systems is appropriate, necessary, or duplicative of existing international standards;

(C) if TEVV standards are considered appropriate, a process for prescribing such standards for critical-impact artificial intelligence systems; and

(D) an outline of standards proposed to be issued, including an estimation of the timeline and sequencing of such standards.

(4) Consultation.—In developing the plan required under paragraph (1), the Secretary shall consult the following:

(A) The National Artificial Intelligence Initiative Office.

(B) The interagency committee established under section 5103 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9413).

(C) The National Artificial Intelligence Advisory Committee.

(D) Industry consensus standards issued by non-governmental standards organizations.

(E) Other departments, agencies, and instrumentalities of the Federal Government, as considered appropriate by the Secretary.

(5) Submission to certification advisory committee.—Upon completing the initial plan required under this subsection and upon completing periodic updates to the plan under paragraph (2), the Secretary shall submit the plan to the advisory committee established under subsection (a) for review.

(6) Submission to committees of Congress.—Upon completing the plan required under this subsection, the Secretary shall submit to the relevant committees of Congress a report containing the plan.

(7) Limitation.—The Secretary may not issue TEVV standards under subsection (c) until the date of the submission of the plan under paragraphs (5) and (6).

(c) Standards.—

(1) Standards.—

(A) In general.—The Secretary shall issue TEVV standards for critical-impact artificial intelligence systems.

(B) Requirements.—Each standard issued under this subsection shall—

(i) be practicable;

(ii) meet the need for safe, secure, and transparent operations of critical-impact artificial intelligence systems;

(iii) with respect to a relevant standard issued by a non-governmental standards organization that is already in place, align with and be interoperable with that standard;

(iv) provide for a mechanism to, not less frequently than once every 2 years, solicit public comment and update the standard to reflect advancements in technology and system architecture; and

(v) be stated in objective terms.

(2) Considerations.—In issuing TEVV standards for critical-impact artificial intelligence systems under this subsection, the Secretary shall—

(A) consider relevant available information concerning critical-impact artificial intelligence systems, including—

(i) transparency reports submitted under section 203(a);

(ii) risk management assessments conducted under section 206(a); and

(iii) any additional information provided to the Secretary pursuant to section 203(a)(1)(B);

(B) consider whether a proposed standard is reasonable, practicable, and appropriate for the particular type of critical-impact artificial intelligence system for which the standard is proposed;

(C) consult with relevant artificial intelligence stakeholders and review industry standards issued by nongovernmental standards organizations;

(D) pursuant to paragraph (1)(B)(iii), consider whether adoption of a relevant standard issued by a nongovernmental standards organization as a TEVV standard is the most appropriate action; and

(E) consider whether the standard takes into account—

(i) transparent, replicable, and objective assessments of critical-impact artificial intelligence system risk, structure, capabilities, and design;

(ii) the risk posed to the public by an applicable critical-impact artificial intelligence system; and

(iii) the diversity of methodologies and innovative technologies and approaches available to meet the objectives of the standard.

(3) Consultation.—Before finalizing a TEVV standard issued under this subsection, the Secretary shall submit the TEVV standard to the advisory committee established under subsection (a) for review.

(4) Public comment.—Before issuing any TEVV standard under this subsection, the

Secretary shall provide an opportunity for public comment.

(5) Cooperation.—In developing a TEVV standard under this subsection, the Secretary may, as determined appropriate, advise, assist, and cooperate with departments, agencies, and instrumentalities of the Federal Government, States, and other public and private agencies.

(6) Effective date of standards.—

(A) In general.—The Secretary shall specify the effective date of a TEVV standard issued under this subsection in the order issuing the standard.

(B) Limitation.—Subject to subparagraph (C), a TEVV standard issued under this subsection may not become effective—

(i) during the 180-day period following the date on which the TEVV standard is issued; and

(ii) more than 1 year after the date on which the TEVV standard is issued.

(C) Exception.—Subparagraph (B) shall not apply to the effective date of a TEVV standard issued under this section if the Secretary—

(i) finds, for good cause shown, that a different effective date is in the public interest; and

(ii) publishes the reasons for the finding under clause (i).

(7) Rule of construction.—Nothing in this subsection shall be construed to authorize the Secretary to impose any requirements on or take any enforcement actions under this section or section 208 relating to a critical-impact AI organization before a TEVV standard relating to those requirements is prescribed.

(d) Exemptions.—

(1) Authority to exempt and procedures.—

(A) In general.—The Secretary may exempt, on a temporary basis, a critical-impact artificial intelligence system from a TEVV standard issued under subsection (c) on terms the Secretary considers appropriate.

(B) Renewal.—An exemption under subparagraph (A)—

(i) may be renewed only on reapplication; and

(ii) shall conform to the requirements of this paragraph.

(C) Proceedings.—

(i) In general.—The Secretary may begin a proceeding to grant an exemption to a critical-impact artificial intelligence system under this paragraph if the critical-impact AI organization that deployed the critical-impact artificial intelligence systems applies for an exemption or a renewal of an exemption.

(ii) Notice and comment.—The Secretary shall publish notice of the application under clause (i) and provide an opportunity to comment.

(iii) Filing.—An application for an exemption or for a renewal of an exemption under this paragraph shall be filed at such time and in such manner and contain such information as the Secretary may require.

(D) Actions.—The Secretary may grant an exemption under this paragraph upon finding that—

(i) the exemption is consistent with the public interest and this section; and

(ii) the exemption would facilitate the development or evaluation of a feature or characteristic of a critical-impact artificial intelligence system providing a safety and security level that is not less than the TEVV standard level.

(2) Disclosure.—Not later than 30 days after the date on which an application is filed under this subsection, the Secretary may make public information contained in the application or relevant to the application, unless the information concerns or is related to a trade secret or other confidential information not relevant to the application.

(3) Notice of decision.—The Secretary shall publish in the Federal Register a notice of each decision granting or denying an exemption under this subsection and the reasons for granting or denying that exemption, including a justification with supporting information for the selected approach.

(e) Self-certification of Compliance.—

(1) In general.—Subject to paragraph (2), with respect to each critical-impact artificial intelligence system of a critical-impact AI organization, the critical-impact AI organization shall certify to the Secretary that the critical-impact artificial intelligence system complies with applicable TEVV standards issued under this section.

(2) Exception.—A critical-impact AI organization may not issue a certificate under paragraph (1) if, in exercising reasonable care, the critical-impact AI organization has constructive knowledge that the certificate is false or misleading in a material respect.

(f) Noncompliance Findings and Enforcement Action.—

(1) Finding of noncompliance by secretary.—Upon learning that a critical-impact artificial intelligence system deployed by a critical-impact AI organization does not comply with the requirements under this section, the Secretary shall—

(A) immediately—

(i) notify the critical-impact AI organization of the finding; and

(ii) order the critical-impact AI organization to take remedial action to address the noncompliance of the artificial intelligence system; and

(B) may, as determined appropriate or necessary by the Secretary, and if the Secretary determines that actions taken by a critical-impact AI organization are insufficient to remedy the noncompliance of the critical-impact AI organization with this section, take enforcement action under section 208.

(2) Actions by critical-impact ai organization.—If a critical-impact AI organization finds that a critical-impact artificial intelligence system deployed by the critical-impact AI organization is noncompliant with an applicable TEVV standard issued under this section or the critical-impact AI organization is notified of noncompliance by the Secretary under paragraph (1)(A)(i), the critical-impact AI organization shall—

(A) without undue delay, notify the Secretary by certified mail or electronic mail of the noncompliance or receipt of the notification of noncompliance;

(B) take remedial action to address the noncompliance; and

(C) not later than 10 days after the date of the notification or receipt under subparagraph (A), submit to the Secretary a report containing information on—

(i) the nature and discovery of the noncompliant aspect of the critical-impact artificial intelligence system;

(ii) measures taken to remedy such noncompliance; and

(iii) actions taken by the critical-impact AI organization to address stakeholders affected by such noncompliance.

SEC. 208. ENFORCEMENT.

(a) In General.—Upon discovering noncompliance with a provision of this Act by a deployer of a high-impact artificial intelligence system or a critical-impact AI organization if the Secretary determines that actions taken by the critical-impact AI organization are insufficient to remedy the noncompliance, the Secretary shall take an action described in this section.

(b) Civil Penalties.—

(1) In general.—The Secretary may impose a penalty described in paragraph (2) on deployer of a high-impact artificial intelligence system or a critical-impact AI organization for each violation by that entity of this Act or any regulation or order issued under this Act.

(2) Penalty described.—The penalty described in this paragraph is the greater of—

(A) an amount not to exceed $300,000; or

(B) an amount that is twice the value of the transaction that is the basis of the violation with respect to which the penalty is imposed.

(c) Violation With Intent.—

(1) In general.—If the Secretary determines that a deployer of a high-impact artificial intelligence system or a critical-impact AI organization intentionally violates this Act or any regulation or order issued under this Act, the Secretary may prohibit the critical-impact AI organization from deploying a critical-impact artificial intelligence system.

(2) In addition .—A prohibition imposed under paragraph (1) shall be in addition to any other civil penalties provided under this Act.

(d) Factors.—The Secretary may by regulation provide standards for establishing levels of civil penalty under this section based upon factors such as the seriousness of the violation, the culpability of the violator, and such mitigating factors as the violator's record of cooperation with the Secretary in disclosing the violation.

(e) Civil Action.—

(1) In general.—Upon referral by the Secretary, the Attorney General may bring a civil action in a United States district court to—

(A) enjoin a violation of section 207; or

(B) collect a civil penalty upon a finding of noncompliance with this Act.

(2) Venue.—A civil action may be brought under paragraph (1) in the judicial district in which the violation occurred or the defendant is found, resides, or does business.

(3) Process.—Process in a civil action under paragraph (1) may be served in any judicial district in which the defendant resides or is found.

(f) Rule of Construction.—Nothing in this section shall be construed to require a developer of a critical-impact artificial intelligence system to disclose any information, including data or algorithms—

(1) relating to a trade secret or other protected intellectual property right;

(2) that is confidential business information; or

(3) that is privileged.

SEC. 209. ARTIFICIAL INTELLIGENCE CONSUMER EDUCATION.

(a) Establishment.—Not later than 180 days after the date of enactment of this Act, the Secretary shall establish a working group relating to responsible education efforts for artificial intelligence systems.

(b) Membership.—

(1) In general.—The Secretary shall appoint to serve as members of the working group established under this section not more than 15 individuals with expertise relating to artificial intelligence systems, including—

(A) representatives of—

(i) institutions of higher education;

(ii) companies developing or operating artificial intelligence systems;

(iii) consumers or consumer advocacy groups;

(iv) public health organizations;

(v) marketing professionals;

(vi) entities with national experience relating to consumer education, including technology education;

(vii) public safety organizations;

(viii) rural workforce development advocates;

(ix) enabling technology companies; and

(x) nonprofit technology industry trade associations; and

(B) any other members the Secretary considers to be appropriate.

(2) COMPENSATION.—A member of the working group established under this section shall serve without compensation.

(c) DUTIES.—

(1) IN GENERAL.—The working group established under this section shall—

(A) identify recommended education and programs that may be voluntarily employed by industry to inform—

(i) consumers and other stakeholders with respect to artificial intelligence systems as those systems—

(I) become available; or

(II) are soon to be made widely available for public use or consumption; and

(B) submit to Congress, and make available to the public, a report containing the findings and recommendations under subparagraph (A).

(2) FACTORS FOR CONSIDERATION.—The working group established under this section shall take into consideration topics relating to—

(A) the intent, capabilities, and limitations of artificial intelligence systems;

(B) use cases of artificial intelligence applications that improve lives of the people of the United States, such as improving government efficiency, filling critical roles, and reducing mundane work tasks;

(C) artificial intelligence research breakthroughs;

(D) engagement and interaction methods, including how to adequately inform consumers of interaction with an artificial intelligence system;

(E) human-machine interfaces;

(F) emergency fallback scenarios;

(G) operational boundary responsibilities;

(H) potential mechanisms that could change function behavior in service; and

(I) consistent nomenclature and taxonomy for safety features and systems.

(3) CONSULTATION.—The Secretary shall consult with the Chair of the Federal Trade Commission with respect to the recommendations of the working group established under this section, as appropriate.

(d) TERMINATION.—The working group established under this section shall terminate on the date that is 2 years after the date of enactment of this Act.

By Ms. COLLINS (for herself and Mr. CARDIN):

S. 3326. A bill to improve access to opioid use disorder treatment services under the Medicare program; to the Committee on Finance.

Ms. COLLINS. Madam President, I rise to introduce the Supporting Seniors with Opioid Use Disorder Act with my colleague from Maryland, Senator CARDIN. I very much appreciate his leadership on this issue. The United States is experiencing an opioid overdose and addiction crisis with devastating effects on communities across the country. The opioid epidemic is claiming the lives of far too many people, with a record 716 Mainers and nearly 110,000 Americans lost in 2022. While many perceive the face of opioid addiction as young, the epidemic harms older adults as well. In Maine, approximately 12 percent of drug overdose deaths last year were among residents age 60 and older.

Each and every opioid death is preventable, and more can be done to ensure that the unique needs of older Americans struggling with addiction are not forgotten. In December 2021, the Department of Health and Human Services Office of the Inspector General, OIG, identified an urgent need to increase the number of Medicare beneficiaries receiving treatment for opioid use disorder. The legislation we are introducing today would help improve seniors' awareness of, and access to, opioid use disorder, OUD, treatment covered by the Medicare Program.

The challenges of the pandemic, combined with the increased prevalence of fentanyl entering our country, have aggravated this national crisis. Even before COVID–19, however, the number of people age 55 or older treated in emergency rooms for nonfatal opioid overdoses was increasing, with a shocking 32 percent jump in ER visits from 2016 to 2017. In 2018, when I served as chairman of the Senate Special Committee on Aging, I chaired a hearing on this topic to shed light on the unique challenges faced by this often-overlooked population. One expert witness told the Aging Committee, ''Medicare beneficiaries are the fastest growing population of diagnosed opioid use disorders.'' Dr. Charles Pattavina, an emergency medicine physician in Bangor, ME, also explained how increased incidences of acute illnesses and injuries among older Americans make them more susceptible to opioid misuse.

In 2021, the Office of the Inspector General investigated the extent to which Medicare beneficiaries diagnosed with opioid use disorder received medication and behavioral therapy through Medicare. The report found that more than 1 million Medicare beneficiaries were diagnosed with OUD in 2020, yet fewer than 16 percent of those patients received medication to treat their OUD. The report also concluded that older beneficiaries were three times less likely to receive medication to treat their OUD than younger beneficiaries. Even fewer beneficiaries received both medication and behavioral therapy. The conclusion was clear: Medicare beneficiaries are not receiving the OUD treatment they need.

A followup OIG report from September 2022 revealed that the situation has largely failed to improve over time. About 50,400 Part D beneficiaries experienced an opioid overdose—from prescription opioids, illicit opioids, or both—during 2021. While the overall proportion of beneficiaries with opioid use disorder receiving medication increased slightly from 16 percent in 2020 to 18 percent in 2021, still fewer than one in five Medicare beneficiaries received the medication they need. This report echoed the call to implement the 2021 OIG recommendations.

The Supporting Seniors with Opioid Use Disorder Act would put into law the recommendations made by the HHS OIG regarding how to improve beneficiaries' awareness of Medicare coverage for OUD treatment and how to identify gaps and opportunities to better meet the needs of this unique population. Specifically, our legislation would require CMS to conduct additional outreach to beneficiaries to increase awareness about Medicare coverage for the treatment of OUD, such as by revising enrollment materials, making State and national contact information for healthcare providers publicly available and easily accessible, and developing or improving continuing education programs about opioid medications and substance use disorder treatment programs. Our bill would also improve data sharing within Agencies at HHS with the goal of obtaining a better understanding of current treatment gaps.

Finally, the bill would require HHS to convene a stakeholder meeting to share best practices on the use of behavioral therapy among beneficiaries receiving medication to treat opioid use disorder. Emerging research points to evidence that patients receiving medication to treat opioid use disorder may also benefit from behavioral therapy, so this opportunity for collaboration on strategies to support better treatment engagement and continuity could be beneficial to both patients and healthcare professionals.

The drug crisis continues to ravage our country, and it is critical that people who are suffering from opioid use disorder have access to the treatment they need to survive and thrive—including our seniors. Challenges in treatment and recovery will persist, but we can begin by better supporting older Americans' access to opioid use disorder services and by strengthening our understanding of potential disparities in treatment. I urge my colleagues to support this important legislation.

By Mr. DURBIN (for himself, Mr. GRAHAM, Mr. WHITEHOUSE, Mr. CORNYN, Ms. KLOBUCHAR, Mr. KENNEDY, Mr. BLUMENTHAL, Mr. TILLIS, and Ms. HIRONO):

S. 3328. A bill to exempt for an additional 4-year period, from the application of the means-test presumption of abuse under chapter 7, qualifying members of reserve components of the Armed Forces and members of the National Guard who, after September 11, 2001, are called to active duty or to perform a homeland defense activity for not less than 90 days; to the Committee on the Judiciary.

Mr. DURBIN. Madam President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the text of the bill was ordered to be printed in the RECORD, as follows:

S. 3328

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Guard and Reservists Debt Relief Extension Act of 2023''.

SEC. 2. NATIONAL GUARD AND RESERVISTS DEBT RELIEF AMENDMENT.

Section 4(b) of the National Guard and Reservists Debt Relief Act of 2008 (Public Law 110–438; 122 Stat. 5000) is amended by striking ‘‘15-year’’ and inserting ‘‘19-year’’.

SUBMITTED RESOLUTIONS

SENATE RESOLUTION 464—SUPPORTING THE GOALS AND PRINCIPLES OF TRANSGENDER DAY OF REMEMBRANCE BY RECOGNIZING THE EPIDEMIC OF VIOLENCE TOWARD TRANSGENDER PEOPLE AND MEMORIALIZING THE LIVES LOST THIS YEAR

Ms. HIRONO (for herself, Ms. BALDWIN, Ms. BUTLER, Mr. FETTERMAN, Mr. MARKEY, Ms. WARREN, Mr. WYDEN, Mr. MERKLEY, and Mr. SCHATZ) submitted the following resolution; which was referred to the Committee on the Judiciary:

S. RES. 464

Whereas Transgender Day of Remembrance was created following the 1998 killing of Rita Hester, a transgender woman of color, whose murder has yet to be solved;

Whereas the following year, on November 20, 1999, Gwendolyn Ann Smith created the first Transgender Day of Remembrance in honor of Rita Hester and other transgender people whose lives were lost due to violence;

Whereas Transgender Day of Remembrance 2023 honors the memory of the lives of transgender people tragically lost in acts of violence between October 1, 2022, and September 30, 2023;

Whereas the United States is currently experiencing an epidemic of violence against transgender people of the United States;

Whereas at least 33 transgender or gender nonconforming people were violently killed in the United States in 2023, a number many believe to be much higher due to the prevalence of underreporting or misreporting violence against this community;

Whereas the lives of Tiffany Banks, Kelly Loving, Daniel Aston, Diamond Jackson-McDonald, Destiny Howard, Mar'Quis ‘‘MJ’’ Jackson, Caelee Love-Light, Jasmine ‘‘Star’’ Mack; KC Johnson, Unique Banks, Zachee Imanitwitaho, Maria Jose Rivera Rivera, Chashay Ashanti Henderson, Paris Aminah, Tortuguita, Ta'Ssiyah Woodland, Ashley Burton, Koko Da Doll, Banko Brown, Ashia Davis, Chanell Perez Ortiz, Jacob Williamson, Camdyn Rider, DéVonnie J'Rae Johnson, Thomas ‘‘Tom-Tom’’ Robertson, YOKO, Luis Ángel Díaz Castro, Sherlyn Marjorie, Emma Borhanian, Clayton Stephens, Ome Gandhi, Lovely Page, Bre'Asia Banks, and Alexa Sokova were tragically lost in acts of violence between October 1, 2022, and September 30, 2023;

Whereas, following the introduction of the Transgender Day of Remembrance Resolution of 2022, the lives of Morgan Moore, Kylie Monali, and London Starr were reported to have been lost to acts of violence between October 1, 2021, and September 30, 2022;

Whereas at least 285 transgender or gender nonconforming people have been murdered worldwide in 2023, according to the Transgender Day of Remembrance memorial page from Trans Lives Matter;

Whereas violence against transgender people of the United States disproportionately impacts transgender women of color;

Whereas Black transgender women are the most targeted group to experience violence in the United States;

Whereas the COVID–19 global health pandemic has had a disproportionate impact on transgender people of the United States;

Whereas transgender people of the United States face barriers to health care, such as lack of health insurance, stigma and discrimination, and higher rates of unemployment;

Whereas transgender people disproportionately suffer from higher rates of homelessness, with reports suggesting as many as ⅓ of all transgender women and ½ of transgender women who are Black, Middle Eastern, multiracial, or undocumented have experienced homelessness;

Whereas almost half of all transgender people in the United States will attempt suicide at least once, and over 1 in 20 will attempt suicide each year, a rate that is almost 10 times higher than the rest of the United States population;

Whereas asylum seekers and refugees who are transgender experience disproportionate rates of violence, including sexual violence, as they seek safety;

Whereas transgender immigrants have died in detention centers in the United States due to medical neglect, injury, and abuse at the hands of staff;

Whereas transgender people who are housed in institutional settings such as jails and prisons are subject to high levels of violence and discrimination;

Whereas transgender students are significantly more likely to experience bullying and harassment at school due to their gender identity;

Whereas understanding and addressing the challenges faced by transgender people of the United States is hampered by a severe lack of data;

Whereas Congress and the executive branch must act to protect and preserve the lives of all people of the United States, including those that are transgender, through inclusive legislation and policies that treat everyone with dignity and respect;

Whereas the continued introduction of anti-transgender legislation has fueled violence against transgender people of the United States;

Whereas the pressure some State legislatures have pushed on State and local authorities to treat gender-affirming health care as child abuse has led to a spike in bullying and assault in schools, worsening mental health among transgender youth and adults, and parents who are afraid their children will be deprived of medical care or be removed from their homes;

Whereas the transgender community has shown great resilience in the face of adversity in all aspects of their lives, including housing, education, employment, and health care; and

Whereas the transgender community has demonstrated tremendous leadership since the courageous actions of many community members, including Marsha P. Johnson and Sylvia Rivera, at the Stonewall uprising of 1969: Now, therefore, be it

Resolved, That the Senate—

(1) supports the goals and principles of Transgender Day of Remembrance by recognizing the epidemic of violence toward transgender people and memorializing the lives lost this year;

(2) recognizes that the alarming trends of increased violence against transgender people of the United States, particularly transgender women of color, are unacceptable, and that finding solutions to these issues must be a pressing priority for the United States Government;

(3) supports efforts to study, respond to, and prevent violence against transgender people;

(4) affirms the principle that every person is endowed with basic human rights and that the commitment of the United States to this principle must encompass every single individual;

(5) recognizes the bravery and resilience of the transgender community as it fights for equal dignity and respect; and

(6) recognizes the multitude of contributions and cultural impact the transgender community has had on the society of the United States.

SENATE RESOLUTION 465—EXPRESSING SUPPORT FOR THE DESIGNATION OF NOVEMBER 20, 2023, THROUGH DECEMBER 20, 2023, AS ‘‘NATIONAL SURVIVORS OF HOMICIDE VICTIMS AWARENESS MONTH’’

Mr. MARKEY submitted the following resolution; which was referred to the Committee on the Judiciary.:

S. RES. 465

Whereas the United States faces a national public health crisis of gun violence;

Whereas, on average, more than 13,000 homicides each year continue to rob families and communities of loved ones;

Whereas homicides increased by 30 percent in 2020, compounding the many deaths caused by COVID–19;

Whereas for every 1 homicide victim, there are at least 10 surviving family members, and the number of survivors of homicide victims grows exponentially each year as they navigate life after the tragic loss of their loved one;

Whereas homicide victims are loved and grieved by family members, friends, neighbors, classmates, colleagues, and communities across the country;

Whereas, in the United States, almost 1 in 4 Black American, Hispanic, or Latinx adults report having lost a loved one to gun-related homicide;

Whereas losing a loved one to homicide is one of the most traumatic events a person can experience;

Whereas, in the United States, homicide is the leading cause of death among Black Americans between the ages of 12–19 and the second leading cause of death for teenagers nationwide;

Whereas more than ½ of women who are victims of homicides are killed because of intimate partner violence;

Whereas 40 percent of homicides in the United States go unsolved;

Whereas homicide results in chronic physical and behavioral health consequences that carry significant behavioral and economic burdens on families and communities impacted by murder, trauma, grief, and loss;

Whereas all families of homicide victims deserve to be treated with dignity and compassion;

Whereas surviving family members need holistic, coordinated, compassionate, and consistent support and services in the immediate aftermath of a homicide and ongoing opportunities for healing in the months and years afterward;

Whereas surviving family members want to remember and honor their loved ones' lives regardless of the circumstances surrounding their death;

Whereas survivors of homicide victims are transforming their pain into purpose by informing, influencing, and impacting public policy, and working to create and sustain an environment where all families can live in peace and all people are valued;

Whereas survivors, advocates, and providers are working together to implement