S-3753.4

SENATE BILL 6284

State of Washington 69th Legislature 2026 Regular Session

By Senators Liias, Boehnke, Shewmake, and Harris

AN ACT Relating to consumer protections for artificial intelligence systems; amending 2024 c 163 s 2 (uncodified); adding a new chapter to Title 19 RCW; adding a new chapter to Title 42 RCW; creating a new section; and providing expiration dates.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec. 1.** The legislature finds that artificial intelligence is a dynamic technology that is changing the way Washingtonians live, learn, and work. Emerging artificial intelligence technologies seek to enhance information gathering and decision making, create new efficiencies throughout the economy, and advance scientific discovery. The legislature also recognizes that there are potential risks associated with the rapid development and deployment of artificial intelligence systems, including the generation of bias and unintentional discrimination. These risks are especially profound when an artificial intelligence system is used to make decisions that have a material or legal impact on someone's life.

The legislature recognizes Washington's role as a leader and innovator within the high-technology economy. The legislature intends to adopt an artificial intelligence regulatory framework that continues to promote innovation, reduce risk, and protect residents

from discriminatory actions. The legislature further recognizes that regulatory frameworks that align with national standards and specify clear compliance requirements provide developers with certainty to support continued innovation while also protecting consumers from unfair or unclear artificial intelligence decisions.

Therefore, it is the intent of the legislature to protect Washingtonians from algorithmic discrimination by establishing a comprehensive risk-based approach to artificial intelligence accountability. The legislature intends to regulate deployers of artificial intelligence under the presumption that they are acting in good faith when they comply with the provisions of this act. The legislature also intends to ensure that government agencies are transparent and accountable by requiring disclosure when consumer interactions are supported by an artificial intelligence system. Finally, the legislature intends to extend and expand the work of the artificial intelligence task force to develop a framework for the adoption of artificial intelligence in the workplace in a way that centers workers and protects fairness and opportunity.

NEW SECTION. **Sec. 2.** The definitions in this section apply throughout this chapter unless the context clearly requires otherwise.

(1) "Algorithmic discrimination":

(a) Means the use of an artificial intelligence system which results in any unlawful differential impact that disfavors any individual or group of individuals on the basis of chapter 49.60 RCW or federal law; and

(b) Does not include the following:

(i) Any offer, license, or use of a high-risk artificial intelligence system by a developer or deployer for the sole purpose of: (A) The developer's or deployer's testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with state and federal law; or (B) expanding an applicant, customer, or participant pool to increase diversity or redress historic discrimination; or

(ii) Any act or omission by or on behalf of a private club or other establishment not in fact open to the public, as set forth in Title II of the Civil Rights Act of 1964, 42 U.S.C. Sec. 2000a(e), as amended.

(2) "Artificial intelligence" means the use of machine learning and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, speech or natural language processing, and content generation.

(3) "Consequential decision" means any decision that has a material legal or similarly significant effect on the provision or denial of any consumer's access to:

(a) Pardon, parole, probation, or release;

(b) Education enrollment or opportunity;

(c) Employment;

(d) A financial or lending service;

(e) An essential government service;

(f) Health care services;

(g) Housing;

(h) Insurance; or

(i) Legal service.

(4) "Consumer" means any individual who is a resident of this state.

(5) "Deploys" or "deployed" means to put a high-risk artificial intelligence system into use.

(6) "Deployer" means any person doing business in this state that deploys a high-risk artificial intelligence system in the state.

(7) "Developer" means any person doing business in this state that develops, or intentionally and substantially modifies, a high-risk artificial intelligence system intended for use within the state.

(8) "High-risk artificial intelligence system":

(a) Means any artificial intelligence system designed by its developer to, when deployed, make, or is a substantial factor in making, a consequential decision; and

(b) Does not include:

(i) Any artificial intelligence system that is intended to:

(A) Perform any narrow procedural task;

(B) Improve the result of a previously completed human activity;

(C) Perform a preparatory task to an assessment relevant to a consequential decision; or

(D) Detect any decision-making pattern, or any deviation from any preexisting decision-making pattern;

(ii) Any antifraud technology, antimalware, antivirus, calculator, cybersecurity, database, data storage, firewall, internet domain registration, internet website loading, networking, robocall-filtering, spam-filtering, spellchecking, spreadsheet, webcaching, webhosting, search engine, or similar technology; or

(iii) Any technology that communicates in natural language for the purpose of providing users with information, making referrals or recommendations, answering questions, or generating other content, and is subject to an acceptable use policy that prohibits generating content that is unlawful.

(9) "Intentional and substantial modification" or "intentionally and substantially modifies" means a deliberate change made to an artificial intelligence system that materially increases the risk of algorithmic discrimination.

(10) "Person" means any individual, association, corporation, limited liability company, partnership, trust, or other legal entity.

(11) "Substantial factor" means a factor that is:

(a) Considered when making a consequential decision;

(b) Likely to alter the outcome of a consequential decision; and

(c) Weighed more heavily by a deployer of the applicable high-risk artificial intelligence system than any other factor contributing to the consequential decision.

NEW SECTION. **Sec. 3.** (1)(a) Beginning July 1, 2027, each deployer of a high-risk artificial intelligence system must use industry-standard means to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination.

(b) In any enforcement action brought on or after July 1, 2027, by the attorney general pursuant to section 9 of this act, there is a rebuttable presumption that a deployer of a high-risk artificial intelligence system used reasonable care as required under this section if the deployer complied with this chapter.

(2)(a) By July 1, 2027, and at least annually thereafter, a deployer or third party contracted by the deployer shall review the deployment of each high-risk artificial intelligence system deployed by the deployer to ensure that the high-risk artificial intelligence system is not causing algorithmic discrimination.

(b) If a deployer subsequently discovers that the high-risk artificial intelligence system has caused algorithmic discrimination, the deployer, without unreasonable delay, but no later than 90 days

after the date of the discovery, shall send to the attorney general, in a form and manner prescribed by the attorney general, a notice disclosing the discovery.

(3) Nothing in this section may be construed to require a deployer to disclose any trade secret, or other confidential or proprietary information.

NEW SECTION. **Sec. 4.** (1) Beginning July 1, 2027, and except as provided in section 5(6) of this act, each deployer of a high-risk artificial intelligence system shall implement and maintain a risk management policy and program to govern the deployer's deployment of a high-risk artificial intelligence system.

(2)(a) The risk management policy and program must specify and incorporate the principles, processes, and personnel that the deployer uses to identify, document, and mitigate known or reasonably foreseeable risks of algorithmic discrimination. The risk management policy and program must include an iterative process that is planned, implemented, and regularly and systematically reviewed and updated over the lifecycle of the high-risk artificial intelligence system.

(b) A risk management policy and program implemented and maintained pursuant to this subsection must be reasonable, considering:

(i) The size and complexity of the deployer;

(ii) The nature and scope of the high-risk artificial intelligence systems deployed by the deployer including, but not limited to, the intended uses of such high-risk artificial intelligence systems;

(iii) The sensitivity and volume of data processed in connection with the high-risk artificial intelligence systems deployed by the deployer; and

(iv) A risk management framework that either:

(A) Adheres to the guidance and standards set forth in the latest version of the artificial intelligence risk management framework published by the national institute of standards and technology, ISO/IEC 42001, or another nationally or internationally recognized risk management framework for artificial intelligence systems, if the standards are substantially equivalent to or more stringent than the requirements; or

(B) Complies with any risk management framework for artificial intelligence systems that the attorney general, in the attorney general's discretion, may designate.

(c) A risk management policy and program implemented and maintained pursuant to this subsection (2) may cover multiple high-risk artificial intelligence systems deployed by the deployer.

(3) Nothing in this section may be construed to require a deployer to disclose any trade secret, or other confidential or proprietary information.

NEW SECTION. **Sec. 5.** (1) Except as provided in subsection (6) of this section, a deployer that deploys a high-risk artificial intelligence system on or after July 1, 2027, or a third party contracted by the deployer for such purposes, shall complete an impact assessment for:

(a) The high-risk artificial intelligence system; and

(b) A deployed high-risk artificial intelligence system no later than 90 days after any intentional and substantial modification to such high-risk artificial intelligence system is made available.

(2) Each impact assessment completed pursuant to this section must include, at a minimum, and to the extent reasonably known by, or available to, the deployer:

(a) A statement by the deployer disclosing the purpose, intended use cases and deployment context of, and benefits afforded by, the high-risk artificial intelligence system;

(b) An analysis of whether the deployment of the high-risk artificial intelligence system poses any known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature of such algorithmic discrimination and the steps that have been taken to mitigate such risks;

(c) A description of the following:

(i) The categories of data the high-risk artificial intelligence system processes as inputs;

(ii) The outputs the high-risk artificial intelligence system produces;

(iii) Any metrics used to evaluate the performance and known limitations of the high-risk artificial intelligence system;

(iv) A description of any transparency measures taken concerning the high-risk artificial intelligence system, such as any measures taken to disclose to a consumer that such high-risk artificial

intelligence system is in use when such high-risk artificial intelligence system is in use; and

(v) A description of the postdeployment monitoring and user safeguards provided concerning such high-risk artificial intelligence system, such as the oversight process established by the deployer to address issues arising from deployment of such high-risk artificial intelligence system.

(3) In addition to the information required under subsection (2)(c) of this section, each impact assessment completed following an intentional and substantial modification made to a high-risk artificial intelligence system on or after July 1, 2027, must include a statement disclosing the extent to which the high-risk artificial intelligence system was used in a manner that was consistent with, or varied from, the developer's intended uses of such high-risk artificial intelligence system.

(4) A single impact assessment may address a comparable set of high-risk artificial intelligence systems deployed by a deployer.

(5) If a deployer, or a third party contracted by the deployer, completes an impact assessment for the purpose of complying with another applicable law or regulation, such impact assessment satisfies the requirements established in this section if such impact assessment is reasonably similar in scope and effect to the impact assessment that would otherwise be completed pursuant to this subsection.

(6) A deployer shall maintain the most recently completed impact assessment for a high-risk artificial intelligence system as required under this section, relevant records supporting the impact assessment, and prior impact assessments, if any, for a period of at least three years following the final deployment of the high-risk artificial intelligence system.

(7) Nothing in this section may be construed to require a deployer to disclose any trade secret, or other confidential or proprietary information.

NEW SECTION. **Sec. 6.** (1) The requirements in section 5 (1) through (3) of this act and section 3(2) of this act do not apply to a deployer if, at the time the deployer deploys a high-risk artificial intelligence system and at all times while the high-risk artificial intelligence system is deployed:

(a) The deployer:

(i) Employs fewer than 50 full-time equivalent employees; and

(ii) Does not use the deployer's own data to train the high-risk artificial intelligence system;

(b) The high-risk artificial intelligence system:

(i) Is used for the intended uses that are disclosed by the deployer; and

(ii) Continues learning based on data derived from sources other than the deployer's own data; and

(c) The deployer makes available to consumers any impact assessment that:

(i) The developer of the high-risk artificial intelligence system has completed and provided to the deployers; and

(ii) Includes information that is substantially similar to the information in the impact assessment required under section 5 of this act.

(2) Nothing in this section may be construed to require a deployer to disclose any trade secret, or other confidential or proprietary information.

NEW SECTION. **Sec. 7.** Beginning July 1, 2026, each time a deployer deploys a high-risk artificial intelligence system to make, or be a substantial factor in making, a consequential decision concerning a consumer, the deployer shall:

(1) Notify the consumer that the deployer has deployed a high-risk artificial intelligence system to make, or be a substantial factor in making, a consequential decision before the decision is made; and

(2) Provide to the consumer a statement disclosing:

(a) The purpose of the high-risk artificial intelligence system and the nature of the consequential decisions;

(b) The contact information for the deployer; and

(c) A description, in plain language, of the high-risk artificial intelligence system.

NEW SECTION. **Sec. 8.** (1) Nothing in this chapter may be construed to:

(a) Restrict a developer's, deployer's, or other person's ability to:

(i) Comply with federal, state, or municipal law;

(ii) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, municipal, or other governmental authorities;

(iii) Cooperate with law enforcement agencies concerning conduct or activity that the developer, deployer, or other person reasonably and in good faith believes may violate federal, state, or municipal law;

(iv) Investigate, establish, exercise, prepare for, or defend legal claims;

(v) Take immediate steps to protect an interest that is essential for the life or physical safety of a consumer or another individual;

(vi) Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is conducted in accordance with 45 C.F.R. Part 46, as amended from time to time, or relevant requirements established by the federal food and drug administration;

(vii) Conduct any research, testing, or development activities regarding any artificial intelligence system or model, other than testing conducted under real world conditions, before such artificial intelligence system or model is placed on the market, deployed, or put into service, as applicable;

(viii) Effectuate a product recall;

(ix) Identify and repair technical errors that impair existing or intended functionality; or

(x) Assist another developer, deployer, or person with any of the obligations imposed under this chapter;

(b) Impose any obligation on a developer, deployer, or other person that adversely affects the rights or freedoms of any person including, but not limited to, the rights of any person to freedom of speech or freedom of the press guaranteed in the First Amendment to the United States Constitution;

(c) Apply to any developer, deployer, or other person:

(i) Insofar as such developer, deployer, or other person develops, deploys, puts into service, or intentionally and substantially modifies, as applicable, a high-risk artificial intelligence system that has been approved, authorized, certified, cleared, or granted:

(A) By a federal agency, such as the federal food and drug administration or the federal aviation administration, acting within the scope of such federal agency's authority; or

(B) In compliance with standards established by any federal agency including, but not limited to, standards established by the federal office of the national coordinator for health information technology;

(ii) Conducting any research to support an application for approval or certification from any federal agency including, but not limited to, the federal aviation administration, the federal communications commission, or the federal food and drug administration, or otherwise subject to review by such federal agency;

(iii) Performing work under, or in connection with, a contract with the United States department of commerce, the United States department of defense, or the national aeronautics and space administration, unless such developer, deployer, or other person is performing such work on a high-risk artificial intelligence system that is used to make, or as a substantial factor in making, a decision concerning employment or housing; or

(iv) That is a covered entity within the meaning of the health insurance portability and accountability act of 1996, P.L. 104-191, and the regulations promulgated thereunder, as both may be amended from time to time, and providing health care recommendations that:

(A) Are generated by an artificial intelligence system;

(B) Require a health care provider to take action to implement such recommendations; and

(C) Are not considered to be high risk; or

(d) Apply to any artificial intelligence system that is acquired by or for the federal government or any federal agency or department including, but not limited to, the United States department of commerce, the United States department of defense, or the national aeronautics and space administration, unless such artificial intelligence system is a high-risk artificial intelligence system that is used to make, or as a substantial factor in making, a decision concerning employment or housing.

(2) If a developer, deployer, or other person engages in any action pursuant to an exemption set forth in this section, the developer, deployer, or other person bears the burden of demonstrating that such action qualifies for such exemption.

NEW SECTION. **Sec. 9.** (1)(a) The attorney general may bring an action in the name of the state, or as parens patriae on behalf of

persons residing in the state, to enforce this chapter. For actions brought by the attorney general to enforce this chapter, a violation of this chapter is an unfair or deceptive act in trade or commerce for the purpose of applying the consumer protection act, chapter 19.86 RCW. An action to enforce this chapter may not be brought under RCW 19.86.090.

(b) The office of the attorney general, before commencing an action under the consumer protection act, chapter 19.86 RCW, must provide 45 days' written notice to a deployer or developer of the alleged violation of this chapter. For the first violation, the developer or deployer may cure the noticed violation within 60 days of receiving the written notice.

(2) Nothing in this chapter may be construed to limit or otherwise affect the obligations of developers and deployers under applicable laws, rules, or regulations relating to data privacy or security.

NEW SECTION. **Sec. 10.** (1) A government agency that makes available an artificial intelligence system intended to interact with consumers must disclose to each consumer, before or at the time of interaction, that the consumer is interacting with an artificial intelligence system. The disclosure must be:

(a) Clear and conspicuously posted;

(b) Written in plain language; and

(c) May not use a dark pattern.

(2) The disclosure may be provided by using a hyperlink to direct a consumer to a separate web page.

(3) A person is required to make the disclosure under subsection (1) of this section regardless of whether it would be obvious to a reasonable consumer that the consumer is interacting with an artificial intelligence system.

NEW SECTION. **Sec. 11.** Sections 1 through 9 of this act constitute a new chapter in Title 19 RCW.

NEW SECTION. **Sec. 12.** Section 10 of this act constitutes a new chapter in Title 42 RCW.

Sec. 13. 2024 c 163 s 2 (uncodified) is amended to read as follows:

(1) ((~~Subject to the availability of amounts appropriated for this specific purpose, a~~)) A task force to assess current uses and trends and make recommendations to the legislature regarding guidelines and potential legislation for the use of artificial intelligence systems is established.

(2) The task force is composed of an executive committee consisting of members as provided in this subsection.

(a) The president of the senate shall appoint one member from each of the two largest caucuses of the senate.

(b) The speaker of the house of representatives shall appoint one member from each of the two largest caucuses of the house of representatives.

(c) The attorney general shall appoint the following members, selecting only individuals with experience in technology policy:

(i) One member from the office of the governor;

(ii) One member from the office of the attorney general;

(iii) One member from Washington technology solutions;

(iv) One member from the Washington state auditor;

(v) One member representing universities or research institutions that are experts in the design and effect of an algorithmic system;

(vi) One member representing private technology industry groups;

(vii) One member representing business associations;

(viii) Three members representing community advocate organizations that represent communities that are disproportionately vulnerable to being harmed by algorithmic bias;

(ix) One member representing the LGBTQ+ community;

(x) One member representing the retail industry;

(xi) One member representing the hospitality industry;

(xii) One member representing statewide labor organizations; and

(xiii) One member representing public safety.

(d) The task force may meet in person or by telephone conference call, videoconference, or other similar telecommunications method, or a combination of such methods.

(e) The executive committee may convene subcommittees to advise the task force on the recommendations and findings set out in subsection (4) of this section.

(i) The executive committee shall define the scope of activity and subject matter focus required of the subcommittees including, but not limited to: Education and workforce development; public safety and ethics; health care and accessibility; labor; government and

public sector efficiency; state security and cybersecurity; consumer protection and privacy; and industry and innovation.

(ii) Subcommittees and their members may be invited to participate on an ongoing, recurring, or one-time basis.

(iii) The executive committee in collaboration with the attorney general shall appoint members to the subcommittees that must be comprised of industry participants, subject matter experts, representatives of federally recognized tribes, or other relevant stakeholders.

(iv) Each subcommittee must contain at least one member possessing relevant industry expertise and at least one member from an advocacy organization that represents communities that are disproportionately vulnerable to being harmed by algorithmic bias including, but not limited to: African American; Hispanic American; Native American; Asian American; Native Hawaiian and Pacific Islander communities; religious minorities; individuals with disabilities; and other vulnerable communities.

(v) Meeting summaries and reports delivered by the subcommittees to the executive committee must be made available on the attorney general's website within 30 days of delivery.

(3) The office of the attorney general must administer and provide staff support for the task force. The office of the attorney general may, when deemed necessary by the task force, retain consultants to provide data analysis, research, recommendations, training, and other services to the task force for the purposes provided in subsection (4) of this section. The office of the attorney general may work with the task force to determine appropriate subcommittees as needed.

(4) The executive committee and subcommittees of the task force shall examine the development and use of artificial intelligence by private and public sector entities and make recommendations to the legislature regarding guidelines and potential legislation for the use and regulation of artificial intelligence systems to protect Washingtonians' safety, privacy, and civil and intellectual property rights. The task force findings and recommendations must include:

(a) A literature review of public policy issues with artificial intelligence, including benefits and risks to the public broadly, historically excluded communities, and other identifiable groups, racial equity considerations, workforce impacts, and ethical concerns;

(b) A review of existing protections under state and federal law for individual data and privacy rights, safety, civil rights, and intellectual property rights, and how federal, state, and local laws relating to artificial intelligence align, differ, conflict, and interact across levels of government;

(c) A recommended set of guiding principles for artificial intelligence use informed by standards established by relevant bodies, including recommending a definition for ethical artificial intelligence and guiding principles;

(d) Identification of high-risk uses of artificial intelligence, including those that may negatively affect safety or fundamental rights;

(e) Opportunities to support and promote the innovation of artificial intelligence technologies through grants and incentives;

(f) Recommendations on appropriate uses of and limitations on the use of artificial intelligence by state and local governments and the private sector;

(g) Recommendations relating to the appropriate and legal use of training data;

(h) Algorithmic discrimination issues which may occur when artificial intelligence systems are used and contribute to unjustified differential treatment or impacts disfavoring people on the basis of race, color, national origin, citizen or immigration status, families with children, creed, religious belief or affiliation, sex, marital status, the presence of any sensory, mental, or physical disability, age, honorably discharged veteran or military status, sexual orientation, gender expression or gender identity, or any other protected class under RCW 49.60.010 and recommendations to mitigate and protect against algorithmic discrimination;

(i) Recommendations on minimizing unlawful discriminatory or biased outputs or applications;

(j) Recommendations on prioritizing transparency so that the behavior and functional components artificial intelligence can be understood in order to enable the identification of performance issues, safety and privacy concerns, biases, exclusionary practices, and unintended outcomes;

(k) Racial equity issues posed by artificial intelligence systems and ways to mitigate the concerns to build equity into the systems;

(l) Civil liberties issues posed by artificial intelligence systems and civil rights and civil liberties protections to be incorporated into artificial intelligence systems;

(m) Recommendations as to how the state should educate the public on the development and use of artificial intelligence, including information about data privacy and security, data collection and retention practices, use of individual data in machine learning, and intellectual property considerations regarding generative artificial intelligence;

(n) A review of protections of personhood, including replicas of voice or likeness, in typical contract structures, and a review of artificial intelligence tools used to support employment decisions;

(o) Proposed state guidelines for the use of artificial intelligence to inform the development, deployment, and use of artificial intelligence systems to:

(i) Retain appropriate human agency and oversight;

(ii) Be subject to internal and external security testing of systems before public release for high-risk artificial intelligence systems;

(iii) Protect data privacy and security;

(iv) Promote appropriate transparency for consumers when they interact with artificial intelligence systems or products created by artificial intelligence; and

(v) Ensure accountability, considering oversight, impact assessment, auditability, and due diligence mechanisms;

(p) A review of existing civil and criminal remedies for addressing potential harms resulting from the use of artificial intelligence systems and recommendations, if needed, for new means of enforcement and remedies; and

(q) Recommendations for establishing an ongoing committee that must study emerging technologies not limited to artificial technology.

(5) The executive committee of the task force must hold its first meeting within 45 days of final appointments to the task force and must meet at least twice each year thereafter. The task force must submit reports to the governor and the appropriate committees of the legislature detailing its findings and recommendations. A preliminary report must be delivered by December 31, 2024, an interim report by December 1, 2025, and a final report by July 1, ((~~2026~~)) 2027.

Meeting summaries must be posted to the website of the attorney general's office within 30 days of any meeting by the task force.

(6) Legislative members of the task force shall be reimbursed for travel expenses in accordance with RCW 44.04.120. Nonlegislative members are not entitled to be reimbursed for travel expenses if they are elected officials or are participating on behalf of an employer, governmental entity, or other organization. Any reimbursement for other nonlegislative members is subject to chapter 43.03 RCW.

(7) To ensure that the task force has diverse and inclusive representation of those affected by its work, task force members, including subcommittee members, whose participation in the task force may be hampered by financial hardship and may be compensated as provided in RCW 43.03.220.

(8) The definitions in this subsection apply throughout this section unless the context clearly requires otherwise.

(a) "Artificial intelligence" means the use of machine learning and related technologies that use data to train statistical models for the purpose of enabling computer systems to perform tasks normally associated with human intelligence or perception, such as computer vision, speech or natural language processing, and content generation.

(b) "Generative artificial intelligence" means an artificial intelligence system that generates novel data or content based on a foundation model.

(c) "Machine learning" means the process by which artificial intelligence is developed using data and algorithms to draw inferences therefrom to automatically adapt or improve its accuracy without explicit programming.

(d) "Training data" means labeled data that is used to teach artificial intelligence models or machine learning algorithms to make proper decisions. Training data may include, but is not limited to, annotated text, images, video, or audio.

(9) This section expires June 30, ((~~2027~~)) 2028.

NEW SECTION. **Sec. 14.** The artificial intelligence workplace advisory group is established for the purpose of developing artificial intelligence policy related to the workplace. The artificial intelligence workplace advisory group shall report to the artificial intelligence task force established in section 2, chapter 163, Laws of 2024 as prescribed in subsection (4) of this section.

(2) The attorney general shall appoint the following members to the artificial intelligence workplace advisory group:

(a) Two members representing different statewide labor organizations;

(b) Two members representing the business community;

(c) One member representing public sector employees;

(d) One member representing private sector employees;

(e) One member representing higher education institutions with expertise in artificial intelligence and the workforce;

(f) One member with expertise in ethics and artificial intelligence; and

(g) Other members as deemed appropriate by the attorney general.

(3) The artificial intelligence workplace advisory group is responsible for developing guiding principles for the use of artificial intelligence in the workplace. At a minimum, the guiding principles must prioritize the responsible and ethical use of artificial intelligence tools in ways that protect an individual's privacy and minimize the risk of bias in the workplace.

(4) The artificial intelligence workplace advisory group shall deliver an interim report on the development of guiding principles for artificial intelligence in the workplace to the artificial intelligence task force by December 1, 2026, and a final report by March 1, 2027. The final report must be included in the artificial intelligence task force's final report as required by section 2(5), chapter 163, Laws of 2024.

(5) This section expires June 30, 2028.

--- END ---