

25104439D

HOUSE BILL NO. 2094

Offered January 13, 2025

Prefiled January 7, 2025

A BILL to amend the Code of Virginia by adding in Title 59.1 a chapter numbered 58, consisting of sections numbered 59.1-607 through 59.1-613, relating to high-risk artificial intelligence; development, deployment, and use; civil penalties.

Patron—Maldonado

Referred to Committee on Communications, Technology and Innovation

Be it enacted by the General Assembly of Virginia:

1. That the Code of Virginia is amended by adding in Title 59.1 a chapter numbered 58, consisting of sections numbered 59.1-607 through 59.1-613, as follows:

CHAPTER 58.

HIGH-RISK ARTIFICIAL INTELLIGENCE DEVELOPER AND DEPLOYER ACT.

§ 59.1-607. Definitions.

As used in this chapter, unless the context requires a different meaning:

"Algorithmic discrimination" means the use of an artificial intelligence system that results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, sexual orientation, veteran status, or other classification protected under state or federal law. "Algorithmic discrimination" does not include (i) the offer, license, or use of a high-risk artificial intelligence system by a developer or deployer for the sole purpose of the developer's or deployer's self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with state and federal law; (ii) the expansion of an applicant, customer, or participant pool to increase diversity or redress historical discrimination; or (iii) an 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. § 2000a(e), as amended from time to time.

"Artificial intelligence system" means any machine learning-based system that, for any explicit or implicit objective, infers from the inputs such system receives how to generate outputs, including content, decisions, predictions, and recommendations, that can influence physical or virtual environments.

"Consequential decision" means any decision that has a material legal, or similarly significant, effect on the provision or denial to any consumer of, or the cost or terms of, (i) parole, probation, a pardon, or any other release from incarceration or supervision, (ii) education enrollment or an education opportunity, (iii) employment, (iv) a financial or lending service, (v) health care services, (vi) housing, (vii) insurance, or (viii) a legal service.

"Consumer" means a natural person who is a resident of the Commonwealth and is acting only in an individual or household context. "Consumer" does not include a natural person acting in a commercial or employment context.

"Deployer" means any person doing business in the Commonwealth that deploys or uses a high-risk artificial intelligence system to make a consequential decision in the Commonwealth.

"Developer" means any person doing business in the Commonwealth that develops or intentionally and substantially modifies a high-risk artificial intelligence system that is offered, sold, leased, given, or otherwise provided to consumers in the Commonwealth.

"Distributor" means a person doing business in the Commonwealth, other than a developer, that makes an artificial intelligence system available in the market.

"Foundation model" means a machine learning model that (i) is trained on broad data at scale, (ii) is designed for generality of output, and (iii) can be adapted to a wide range of distinctive tasks.

"General-purpose artificial intelligence model" means any form of artificial intelligence system that (i) displays significant generality, (ii) is capable of competently performing a wide range of distinct tasks, and (iii) can be integrated into a variety of downstream applications or systems. "General-purpose artificial intelligence model" does not include any artificial intelligence model that is used for development, prototyping, and research activities before such artificial intelligence model is released on the market.

"Generative artificial intelligence" means artificial intelligence capable of emulating the structure and characteristics of input data in order to generate derived synthetic content, including audio, images, text, and videos.

"Generative artificial intelligence system" means any artificial intelligence system or service that incorporates generative artificial intelligence.

59 *"High-risk artificial intelligence system" means any artificial intelligence system that is specifically*
60 *intended to autonomously make, or be a substantial factor in making, a consequential decision. A system or*
61 *service is not a "high-risk artificial intelligence system" if it is intended to (i) perform a narrow procedural*
62 *task, (ii) improve the result of a previously completed human activity, (iii) detect any decision-making*
63 *patterns or any deviations from pre-existing decision-making patterns, or (iv) perform a preparatory task to*
64 *an assessment relevant to a consequential decision. "High-risk artificial intelligence system" does not include*
65 *any of the following technologies:*

66 1. *Anti-fraud technology that does not use facial recognition technology;*

67 2. *Anti-malware technology;*

68 3. *Anti-virus technology;*

69 4. *Artificial intelligence-enabled video games;*

70 5. *Calculators;*

71 6. *Cybersecurity technology;*

72 7. *Databases;*

73 8. *Data storage;*

74 9. *Firewall technology;*

75 10. *Internet domain registration;*

76 11. *Internet website loading;*

77 12. *Networking;*

78 13. *Spam and robocall filtering;*

79 14. *Spell-checking technology;*

80 15. *Spreadsheets;*

81 16. *Web caching;*

82 17. *Web hosting or any similar technology; or*

83 18. *Technology that communicates with consumers in natural language for the purpose of providing users*
84 *with information, making referrals or recommendations, and answering questions and is subject to an*
85 *accepted use policy that prohibits generating content that is discriminatory or harmful.*

86 *"Integrator" means a person that knowingly integrates an artificial intelligence system into a software*
87 *application and places such software application on the market. An "integrator" does not include a person*
88 *offering information technology infrastructure.*

89 *"Intentional and substantial modification" means any deliberate change made to (i) an artificial*
90 *intelligence system that results in any new reasonably foreseeable risk of algorithmic discrimination or (ii) a*
91 *general-purpose artificial intelligence model that affects compliance of the general-purpose artificial*
92 *intelligence model, materially changes the purpose of the general-purpose artificial intelligence model, or*
93 *results in any new reasonably foreseeable risk of algorithmic discrimination. "Intentional and substantial*
94 *modification" does not include any change made to a high-risk artificial intelligence system, or the*
95 *performance of a high-risk artificial intelligence system, if (a) the high-risk artificial intelligence system*
96 *continues to learn after such high-risk artificial intelligence system is offered, sold, leased, licensed, given, or*
97 *otherwise made available to a deployer, or deployed, and (b) such change (1) is made to such high-risk*
98 *artificial intelligence system as a result of any learning described in clause (a), and (2) was predetermined by*
99 *the deployer or the third party contracted by the deployer and concluded and included within the initial*
100 *impact assessment of such high-risk artificial intelligence system as required in § 59.1-609.*

101 *"Machine learning" means the development of algorithms to build data-derived statistical models that are*
102 *capable of drawing inferences from previously unseen data without explicit human instruction.*

103 *"Person" includes any individual, corporation, partnership, association, cooperative, limited liability*
104 *company, trust, joint venture, or any other legal or commercial entity and any successor, representative,*
105 *agent, agency, or instrumentality thereof. "Person" does not include any government or political subdivision.*

106 *"Principal basis" means the use of an output of a high-risk artificial intelligence system to make a*
107 *decision without (i) human review, oversight, involvement, or intervention or (ii) meaningful consideration by*
108 *a human.*

109 *"Red-teaming" means an exercise that is conducted to identify the potential adverse behaviors or*
110 *outcomes of an artificial intelligence system, identify how such behaviors or outcomes occur, and stress test*
111 *the safeguards against such behaviors or outcomes.*

112 *"Significant update" means any new version, new release, or other update to a high-risk artificial*
113 *intelligence system that results in significant changes to such high-risk artificial intelligence system's use*
114 *case or key functionality and that results in any new or reasonably foreseeable risk of algorithmic*
115 *discrimination.*

116 *"Social media platform" means an electronic medium or service where users may create, share, or view*
117 *user-generated content, including videos, photographs, blogs, podcasts, messages, emails, or website profiles*
118 *or locations, and create a personal account.*

119 *"Substantial factor" means a factor that is (i) the principal basis for making a consequential decision, (ii)*

120 capable of altering the outcome of a consequential decision, and (iii) generated by an artificial intelligence
 121 system. "Substantial factor" includes any use of an artificial intelligence system to generate any content,
 122 decision, prediction, or recommendation concerning a consumer that is used as the principal basis to make a
 123 consequential decision concerning the consumer.

124 "Synthetic digital content" means any digital content, including any audio, image, text, or video, that is
 125 produced or manipulated by a generative artificial intelligence system, including a general-purpose artificial
 126 intelligence model.

127 "Trade secret" means information, including a formula, pattern, compilation, program, device, method,
 128 technique, or process, that (i) derives independent economic value, actual or potential, from not being
 129 generally known to, and not being readily ascertainable by proper means by, other persons who can obtain
 130 economic value from its disclosure or use and (ii) is the subject of efforts that are reasonable under the
 131 circumstances to maintain its secrecy.

132 **§ 59.1-608. Operating standards for developers of high-risk artificial intelligence systems.**

133 A. No developer of a high-risk artificial intelligence system shall offer, sell, lease, give, or otherwise
 134 provide to a deployer, or other developer, a high-risk artificial intelligence system unless the developer
 135 makes available to the deployer or other developer:

136 1. A statement disclosing the intended uses of such high-risk artificial intelligence system;

137 2. Documentation disclosing the following:

138 a. The known or reasonably known limitations of such high-risk artificial intelligence system, including
 139 any and all known or reasonably foreseeable risks of algorithmic discrimination arising from the intended
 140 uses of such high-risk artificial intelligence system;

141 b. The purpose of such high-risk artificial intelligence system and the intended benefits and uses of such
 142 high-risk artificial intelligence system;

143 c. A summary describing how such high-risk artificial intelligence system was evaluated for performance
 144 before such high-risk artificial intelligence system was licensed, sold, leased, given, or otherwise made
 145 available to a deployer;

146 d. The measures the developer has taken to mitigate reasonable foreseeable risks of algorithmic
 147 discrimination that the developer knows arises from deployment or use of such high-risk artificial
 148 intelligence system; and

149 e. How an individual can use such high-risk artificial intelligence system and monitor the performance of
 150 such high-risk artificial intelligence system for any risk of algorithmic discrimination;

151 3. Documentation describing (i) how the high-risk artificial intelligence system was evaluated for
 152 performance and for mitigation of algorithmic discrimination before such system was made available to the
 153 deployer; (ii) the data governance measures used to cover the training data sets and the measures used to
 154 examine the suitability of data sources, possible biases of data sources, and appropriate mitigation; (iii) the
 155 intended outputs of the high-risk artificial intelligence system; (iv) the measures the developer has taken to
 156 mitigate known or reasonably foreseeable risks of algorithmic discrimination that may arise from the
 157 reasonably foreseeable deployment of the high-risk artificial intelligence system; and (v) how the high-risk
 158 artificial intelligence system should be used, not be used, and be monitored by an individual when such
 159 system is used to make, or is a substantial factor in making, a consequential decision; and

160 4. Any additional documentation that is reasonably necessary to assist the deployer in understanding the
 161 outputs and monitoring performance of the high-risk artificial intelligence system for risks of algorithmic
 162 discrimination.

163 B. Each developer that offers, sells, leases, gives, or otherwise makes available to a deployer a high-risk
 164 artificial intelligence system shall make available to the deployer, to the extent feasible and necessary,
 165 information and documentation through artifacts such as model cards or impact assessments, and such
 166 documentation and information shall enable the deployer or a third party contracted by the deployer to
 167 complete an impact assessment as required in § 59.1-609.

168 C. A developer that also serves as a deployer for any high-risk artificial intelligence system shall not be
 169 required to generate the documentation required by this section unless such high-risk artificial intelligence
 170 system is provided to an unaffiliated entity acting as a deployer or as otherwise required by law.

171 D. Nothing in this section shall be construed to require a developer to disclose any trade secret.

172 E. High-risk artificial intelligence systems that are in conformity with the latest version of the Artificial
 173 Intelligence Risk Management Framework published by the National Institute of Standards and Technology,
 174 Standard ISO/IEC 42001 of the International Organization for Standardization, or another nationally or
 175 internationally recognized risk management framework for artificial intelligence systems, or parts thereof,
 176 shall be presumed to be in conformity with related requirements set out in this section and in associated
 177 regulations.

178 F. For any disclosure required pursuant to this section, each developer shall, no later than 90 days after
 179 the developer performs an intentional and substantial modification to any high-risk artificial intelligence
 180 system, update such disclosure as necessary to ensure that such disclosure remains accurate.

181 G. 1. Each developer of a high-risk artificial intelligence system, including a general purpose artificial

182 intelligence model, that generates or manipulates synthetic digital content shall ensure that the outputs of
183 such high-risk artificial intelligence system are marked and detectable, in a manner that is detectable by
184 consumers and complies with any applicable accessibility requirements, as synthetic digital content no later
185 than the time that consumers who did not create such outputs first interact with or are exposed to such
186 output;

187 2. If such synthetic digital content is an audio, image, or video format that forms part of an evidently
188 artistic, creative, satirical, fictional analogous work or program, such requirement for marking outputs of
189 high-risk artificial intelligence systems pursuant to subdivision 1 shall be limited to a manner that does not
190 hinder the display or enjoyment of such work or program.

191 3. The marking of outputs required by subdivision 1 shall not apply to (i) synthetic digital content that
192 consists exclusively of text, is published to inform the public on any matter of public interest, or is unlikely to
193 mislead a reasonable person consuming such synthetic digital content or (ii) the outputs of a high-risk
194 artificial intelligence system that performs an assistive function for standard editing, does not substantially
195 alter the input data provided by the developer, or is used to detect, prevent, investigate, or prosecute any
196 crime as authorized by law.

197 **§ 59.1-609. Operating standards for deployers of high-risk artificial intelligence systems.**

198 A. Each deployer of a high-risk artificial intelligence system shall use a reasonable duty of care to protect
199 consumers from any known or reasonably foreseeable risks of algorithmic discrimination. In any
200 enforcement action brought on or after such date by the Attorney General pursuant to § 59.1-613, there shall
201 be a rebuttable presumption that a deployer of a high-risk artificial intelligence system used a reasonable
202 duty of care as required by this subsection if the deployer complied with the requirements of this section.

203 B. No deployer shall deploy or use a high-risk artificial intelligence system to make a consequential
204 decision unless the deployer has designed and implemented a risk management policy and program for such
205 high-risk artificial intelligence system. The risk management policy shall specify the principles, processes,
206 and personnel that the deployer shall use in maintaining the risk management program to identify, mitigate,
207 and document any risk of algorithmic discrimination that is a reasonably foreseeable consequence of
208 deploying or using such high-risk artificial intelligence system to make a consequential decision. Each risk
209 management policy and program designed, implemented, and maintained pursuant to this subsection shall be
210 (i) at least as stringent as the latest version of the Artificial Intelligence Risk Management Framework
211 published by the National Institute of Standards and Technology, Standard ISO/IEC 42001 of the
212 International Organization for Standardization, or another nationally or internationally recognized risk
213 management framework for artificial intelligence systems and (ii) reasonable considering (a) the size and
214 complexity of the deployer; (b) the nature and scope of the high-risk artificial intelligence systems deployed
215 and used by the deployer, including the intended uses of such high-risk artificial intelligence systems; (c) the
216 sensitivity and volume of data processed in connection with the high-risk artificial intelligence systems
217 deployed and used by the deployer; and (d) the cost to the deployer to implement and maintain such risk
218 management program.

219 C. Except as provided in this subsection, no deployer shall deploy or use a high-risk artificial intelligence
220 system to make a consequential decision unless the deployer has completed an impact assessment for such
221 high-risk artificial intelligence system. The deployer shall complete an impact assessment for a high-risk
222 artificial intelligence system (i) before the deployer initially deploys such high-risk artificial intelligence
223 system and (ii) not later than 90 days after each significant update to such high-risk artificial intelligence
224 system is made available.

225 Each impact assessment completed pursuant to this subsection shall include, at a minimum:

226 1. A statement by the deployer disclosing (i) the purpose, intended use cases and deployment context of,
227 and benefits afforded by the high-risk artificial intelligence system and (ii) whether the deployment or use of
228 the high-risk artificial intelligence system poses any known or reasonably foreseeable risk of algorithmic
229 discrimination and, if so, (a) the nature of such algorithmic discrimination and (b) the steps that have been
230 taken, to the extent feasible, to mitigate such risk;

231 2. For each post-deployment impact assessment completed pursuant to this subsection, whether the
232 intended use cases of the high-risk artificial intelligence system as updated were consistent with, or varied
233 from, the developer's intended uses of such high-risk artificial intelligence system;

234 3. A description of (i) the categories of data the high-risk artificial intelligence system processes as inputs
235 and (ii) the outputs such high-risk artificial intelligence system produces;

236 4. If the deployer used data to customize the high-risk artificial intelligence system, an overview of the
237 categories of data the deployer used to customize such high-risk artificial intelligence system;

238 5. A list of any metrics used to evaluate the performance and known limitations of the high-risk artificial
239 intelligence system;

240 6. A description of any transparency measures taken concerning the high-risk artificial intelligence
241 system, including any measures taken to disclose to a consumer that such high-risk artificial intelligence
242 system is in use when such high-risk artificial intelligence system is in use; and

243 7. A description of any post-deployment monitoring performed and user safeguards provided concerning

244 such high-risk artificial intelligence system, including any oversight process established by the deployer to
 245 address issues arising from deployment or use of such high-risk artificial intelligence system as such issues
 246 arise.

247 A single impact assessment may address a comparable set of high-risk artificial intelligence systems
 248 deployed or used by a deployer. High-risk artificial intelligence systems that are in conformity with the latest
 249 version of the Artificial Intelligence Risk Management Framework published by the National Institute of
 250 Standards and Technology, Standard ISO/IEC 42001 of the International Organization for Standardization,
 251 or another nationally or internationally recognized risk management framework for artificial intelligence
 252 systems, or parts thereof, shall be presumed to be in conformity with related requirements set out in this
 253 section and in associated regulations. If a deployer completes an impact assessment for the purpose of
 254 complying with another applicable law or regulation, such impact assessment shall be deemed to satisfy the
 255 requirements established in this subsection if such impact assessment is reasonably similar in scope and
 256 effect to the impact assessment that would otherwise be completed pursuant to this subsection. A deployer
 257 that completes an impact assessment pursuant to this subsection shall maintain such impact assessment and
 258 all records concerning such impact assessment for three years.

259 D. Not later than the time that a deployer uses a high-risk artificial intelligence system to interact with a
 260 consumer, the deployer shall disclose to the consumer that the deployer is interacting with an artificial
 261 intelligence system disclosing (i) the purpose of such high-risk artificial intelligence system, (ii) the nature of
 262 such system, (iii) the nature of the consequential decision, (iv) the contact information for the deployer, and
 263 (v) a description of the artificial intelligence system in plain language of such system.

264 If such consequential decision is adverse to such consumer, the deployer shall provide to the consumer (a)
 265 a statement disclosing the principal reason or reasons for the consequential decision, including (1) the
 266 degree to which and manner in which the high-risk artificial intelligence system contributed to the
 267 consequential decision, (2) the type of data that was processed by such system in making the consequential
 268 decision, and (3) the sources of such data; (b) an opportunity to correct any incorrect personal data that the
 269 high-risk artificial intelligence system processed in making, or as a substantial factor in making, the
 270 consequential decision; and (c) an opportunity to appeal such adverse consequential decision concerning the
 271 consumer arising from the deployment of such system. Any such appeal shall allow for human review, if
 272 technically feasible, unless providing the opportunity for appeal is not in the best interest of the consumer,
 273 including instances in which any delay might pose a risk to the life or safety of such consumer.

274 E. Each deployer shall make available, in a manner that is clear and readily available, a statement
 275 summarizing how such deployer manages any reasonably foreseeable risk of algorithmic discrimination that
 276 may arise from the use or deployment of the high-risk artificial intelligence system.

277 F. For any disclosure required pursuant to this section, each deployer shall, no later than 90 days after
 278 the developer performs an intentional and substantial modification to any high-risk artificial intelligence
 279 system, update such disclosure as necessary to ensure that such disclosure remains accurate.

280 G. Any deployer who performs an intentional and substantial modification to any high-risk artificial
 281 system shall comply with the documentation and disclosure requirements for developers pursuant to
 282 subsections A through F of § 59.1-608.

283 **§ 59.1-610. Operating standards for integrators of high-risk artificial intelligence systems.**

284 Each integrator of a high-risk artificial intelligence system shall develop and adopt an acceptable use
 285 policy, which shall limit the use of the high-risk artificial intelligence system to mitigate known risks of
 286 algorithmic discrimination.

287 Each integrator of a high-risk artificial intelligence system shall provide to the deployer clear,
 288 conspicuous notice of (i) the name or other identifier of the high-risk artificial intelligence system integrated
 289 into a software application provided to the deployer; (ii) the name and contact information of the developer
 290 of the high-risk artificial intelligence system integrated into a software application provided to the deployer;
 291 (iii) whether the integrator has adjusted the model weights of the high-risk artificial intelligence system
 292 integrated into the software application by exposing it to additional data, a summary of the adjustment
 293 process, and how such process and the resulting system were evaluated for risk of algorithmic discrimination
 294 ; (iv) a summary of any other non-substantial modifications made by the integrator; and (v) the integrator's
 295 acceptable use policy.

296 **§ 59.1-611. Operating standards for distributors of high-risk artificial intelligence systems.**

297 Each distributor of a high-risk artificial intelligence system shall use reasonable care to protect
 298 consumers from any known or reasonably foreseeable risks of algorithmic discrimination. If a distributor of a
 299 high-risk artificial intelligence system considers or has reason to consider that a high-risk artificial
 300 intelligence system is not in compliance with any requirement of this chapter, it shall immediately withdraw,
 301 disable, or recall, as appropriate, the high-risk artificial intelligence system from the market until such
 302 system has been brought into compliance with the requirements of this chapter. The distributor shall inform
 303 the developers of the high-risk artificial intelligence system concerned and, where applicable, the deployer of
 304 any such system's noncompliance with this chapter and the withdrawal, disablement, or recall of such system.

305 **§ 59.1-612. Exemptions.**

306 A. Nothing in this chapter shall be construed to restrict a developer's, integrator's, distributor's or
307 deployer's ability to (i) comply with federal, state, or municipal ordinances or regulations; (ii) comply with a
308 civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, local, or other
309 governmental authorities; (iii) cooperate with law-enforcement agencies concerning conduct or activity that
310 the developer, integrator, distributor, or deployer reasonably and in good faith believes may violate federal,
311 state, or local law, ordinances, or regulations; (iv) investigate, establish, exercise, prepare for, or defend
312 legal claims; (v) provide a product or service specifically requested by a consumer; (vi) perform under a
313 contract to which a consumer is a party, including fulfilling the terms of a written warranty; (vii) take steps
314 at the request of a consumer prior to entering into a contract; (viii) take immediate steps to protect an
315 interest that is essential for the life or physical safety of the consumer or another individual; (ix) prevent,
316 detect, protect against, or respond to security incidents, identity theft, fraud, harassment, or malicious or
317 deceptive activities; (x) take actions to prevent, detect, protect against, report, or respond to the production,
318 generation, incorporation, or synthesization of child sex abuse material, or any illegal activity, preserve the
319 integrity or security of systems, or investigate, report, or prosecute those responsible for any such action; (xi)
320 engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all
321 other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review
322 board that determines, or similar independent oversight entities that determine, (a) that the expected benefits
323 of the research outweigh the risks associated with such research and (b) whether the developer, integrator,
324 distributor, or deployer has implemented reasonable safeguards to mitigate the risks associated with such
325 research; (xii) assist another developer, integrator, distributor, or deployer with any of the obligations
326 imposed by this chapter; or (xiii) take any action that is in the public interest in the areas of public health,
327 community health, or population health, but solely to the extent that such action is subject to suitable and
328 specific measures to safeguard the public.

329 B. The obligations imposed on developers, integrators, distributors, or deployers by this chapter shall not
330 restrict a developer's or deployer's ability to (i) conduct internal research to develop, improve, or repair
331 products, services, or technologies; (ii) effectuate a product recall; (iii) identify and repair technical errors
332 that impair existing or intended functionality; or (iv) perform internal operations that are reasonably aligned
333 with the expectations of the consumer or reasonably anticipated based on the consumer's existing
334 relationship with the developer, integrator, or deployer.

335 C. Nothing in this chapter shall be construed to impose any obligation on a developer, integrator,
336 distributor, or deployer to disclose trade secrets or information protected from disclosure by state or federal
337 law.

338 D. The obligations imposed on developers, integrators, distributors, or deployers by this chapter shall not
339 apply where compliance by the developer, integrator, distributor, or deployer with such obligations would
340 violate an evidentiary privilege under federal law or the laws of the Commonwealth.

341 E. Nothing in this chapter shall be construed to impose any obligation on a developer, integrator,
342 distributor, or deployer that adversely affects the legally protected rights or freedoms of any person,
343 including the rights of any person to freedom of speech or freedom of the press guaranteed in the First
344 Amendment to the Constitution of the United States or under the Virginia Human Rights Act (§ 2.2-3900 et
345 seq.).

346 F. The obligations imposed on developers, integrators, distributors, or deployers by this chapter shall not
347 apply to any artificial intelligence system that is acquired by or for the federal government or any federal
348 agency or department, including the U.S. Department of Commerce, the U.S. Department of Defense, and the
349 National Aeronautics and Space Administration, unless such artificial intelligence system is a high-risk
350 artificial intelligence system that is used to make, or is a substantial factor in making, a decision concerning
351 employment or housing.

352 G. For the purposes of this subsection:

353 "Affiliate" means the same as that term is defined in § 6.2-1800.

354 "Bank" means the same as that term is defined in § 6.2-800.

355 "Credit union" means the same as that term is defined in § 6.2-1300.

356 "Federal credit union" means a credit union duly organized under federal law.

357 "Out-of-state bank" means the same as that term is defined in § 6.2-836.

358 "Out-of-state credit union" means a credit union organized and doing business in another state.

359 "Subsidiary" means the same as that term is defined in § 6.2-700.

360 The obligations imposed on developers, integrators, distributors, or deployers by this chapter shall be
361 deemed satisfied for any bank, out-of-state bank, credit union, federal credit union, out-of-state credit union,
362 or any affiliate or subsidiary thereof if such bank, out-of-state bank, credit union, federal credit union,
363 out-of-state credit union, or affiliate or subsidiary is subject to examination by any state or federal prudential
364 regulator under any published guidance or regulations that apply to the use of high-risk artificial intelligence
365 systems and such guidance or regulations (i) impose requirements that are substantially equivalent to, and at
366 least as stringent as, the requirements set forth in this chapter, and (ii) at a minimum, require such bank,

367 out-of-state bank, credit union, federal credit union, out-of-state credit union, or affiliate or subsidiary to (a)
 368 regularly audit such bank's, out-of-state bank's, credit union's, federal credit union's, out-of-state credit
 369 union's, or affiliate's or subsidiary's use of high-risk artificial intelligence systems for compliance with state
 370 and federal anti-discrimination laws and regulations applicable to such bank, out-of-state bank, credit union,
 371 federal credit union, out-of-state credit union, or affiliate or subsidiary and (b) mitigate any algorithmic
 372 discrimination caused by the use of a high-risk artificial intelligence system or any risk of algorithmic
 373 discrimination that is reasonably foreseeable as a result of the use of a high-risk artificial intelligence
 374 system.

375 H. For purposes of this subsection, "insurer" means the same as that term is defined in § 38.2-100.

376 The provisions of this chapter shall not apply to any insurer, or any high-risk artificial intelligence system
 377 developed or deployed by an insurer for use in the business of insurance, if such insurer is regulated and
 378 supervised by the State Corporation Commission or a comparable federal regulating body and subject to
 379 examination by such entity under any existing statutes, rules, or regulations pertaining to unfair trade
 380 practices and unfair discrimination prohibited under Chapter 5 (§ 38.2-500 et seq.) of Title 38.2, or
 381 published guidance or regulations that apply to the use of high-risk artificial intelligence systems and such
 382 guidance or regulations aid in the prevention and mitigation of algorithmic discrimination caused by the use
 383 of a high-risk artificial intelligence system or any risk of algorithmic discrimination that is reasonably
 384 foreseeable as a result of the use of a high-risk artificial intelligence system. Nothing in this chapter shall be
 385 construed to delegate existing regulatory oversight of the business of insurance to any department or agency
 386 other than the Bureau of Insurance of the Virginia State Corporation Commission.

387 I. The provisions of this chapter shall not apply to the development of an artificial intelligence system that
 388 is used exclusively for research, training, testing, or other pre-deployment activities performed by active
 389 participants of any sandbox software or sandbox environment established and subject to oversight by a
 390 designated agency or other government entity and that is in compliance with the provisions of this chapter.

391 J. The provisions of this chapter shall not apply to a developer, integrator, distributor, or deployer, or
 392 other person who develops, deploys, puts into service, or intentionally modifies, as applicable, a high-risk
 393 artificial intelligence system that (i) has been approved, authorized, certified, cleared, developed, or granted
 394 by a federal agency acting within the scope of the federal agency's authority, or by a regulated entity subject
 395 to the supervision and regulation of the Federal Housing Finance Agency or (ii) is in compliance with
 396 standards established by a federal agency or by a regulated entity subject to the supervision and regulation
 397 of the Federal Housing Finance Agency, if the standards are substantially equivalent or more stringent than
 398 the requirements of this chapter.

399 K. The provisions of this chapter shall not apply to a developer, integrator, distributor, deployer, or other
 400 person that is a covered entity within the meaning of the federal Health Insurance Portability and
 401 Accountability Act of 1996 (42 U.S.C. § 1320d et seq.) and the regulations promulgated under such federal
 402 act, as both may be amended from time to time, and is providing (i) health care recommendations that (a) are
 403 generated by an artificial intelligence system and (b) require a health care provider to take action to
 404 implement the recommendations or (ii) services utilizing an artificial intelligence system for an
 405 administrative, financial, quality measurement, security, or performance improvement function.

406 L. If a developer, integrator, distributor, or deployer engages in any action authorized by an exemption
 407 set forth in this section, the developer, integrator, distributor, or deployer bears the burden of demonstrating
 408 that such action qualifies for such exemption.

409 **§ 59.1-613. Enforcement; civil penalty.**

410 A. The Attorney General shall have exclusive authority to enforce the provisions of this chapter.

411 B. Whenever the Attorney General has reasonable cause to believe that any person has engaged in or is
 412 engaging in any violation of this chapter, the Attorney General is empowered to issue a civil investigative
 413 demand. The provisions of § 59.1-9.10 shall apply mutatis mutandis to civil investigative demands issued
 414 pursuant to this section. In rendering and furnishing any information requested pursuant to a civil
 415 investigative demand issued pursuant to this section, a developer, integrator, distributor, or deployer may
 416 redact or omit any trade secrets or information protected from disclosure by state or federal law. To the
 417 extent that any information requested pursuant to a civil investigative demand issued pursuant to this section
 418 is subject to attorney-client privilege or work-product protection, disclosure of such information pursuant to
 419 the civil investigative demand shall not constitute a waiver of such privilege or protection. Any information,
 420 statement, or documentation provided to the Attorney General pursuant to this section shall be exempt from
 421 disclosure under the Virginia Freedom of Information Act (§ 2.2-3700 et seq.).

422 C. Notwithstanding any contrary provision of law, the Attorney General may cause an action to be
 423 brought in the appropriate circuit court in the name of the Commonwealth to enjoin any violation of this
 424 chapter. The circuit court having jurisdiction may enjoin such violation notwithstanding the existence of an
 425 adequate alternative remedy at law. In any action brought pursuant to this chapter, it shall not be necessary
 426 that damages be proved.

427 D. Any person who violates the provisions of this chapter shall be subject to a civil penalty in an amount

428 *not to exceed \$1,000 plus reasonable attorney fees, expenses, and costs, as determined by the court. Any*
429 *person who willfully violates the provisions of this chapter shall be subject to a civil penalty in an amount not*
430 *less than \$1,000 and not more than \$10,000 plus reasonable attorney fees, expenses, and costs, as*
431 *determined by the court. Such civil penalties shall be paid into the Literary Fund.*

432 *E. Each violation of this chapter shall constitute a separate violation and shall be subject to any civil*
433 *penalties imposed under this section.*

434 *F. The Attorney General may require that a developer disclose to the Attorney General any statement or*
435 *documentation described in this chapter if such statement or documentation is relevant to an investigation*
436 *conducted by the Attorney General. The Attorney General may also require that a deployer disclose to the*
437 *Attorney General any risk management policy designed and implemented, impact assessment completed, or*
438 *record maintained pursuant to this chapter if such risk management policy, impact assessment, or record is*
439 *relevant to an investigation conducted by the Attorney General.*

440 *G. In an action brought by the Attorney General pursuant to this section, it shall be an affirmative defense*
441 *that the developer, integrator, distributor, or deployer (i) discovers a violation of any provision of this*
442 *chapter through red-teaming; (ii) no later than 45 days after discovering such violation (a) cures such*
443 *violation and (b) provides notice to the Attorney General in a form and manner as prescribed by the Attorney*
444 *General that such violation has been cured and evidence that any harm caused by such violation has been*
445 *mitigated; and (iii) is otherwise in compliance with the requirements of this chapter.*

446 *H. Prior to causing an action against a developer, integrator, distributor, or deployer for a violation of*
447 *this chapter pursuant to subsection C, the Attorney General shall determine, in consultation with the*
448 *developer, integrator, distributor, or deployer, if it is possible to cure the violation. If it is possible to cure*
449 *such violation, the Attorney General may issue a notice of violation to the developer, integrator, distributor,*
450 *or deployer and afford the developer, integrator, distributor, or deployer the opportunity to cure such*
451 *violation within 45 days of the receipt of such notice of violation. In determining whether to grant such*
452 *opportunity to cure such violation, the Attorney General shall consider (i) the number of violations, (ii) the*
453 *size and complexity of the developer, integrator, distributor, or deployer; (iii) the nature and extent of the*
454 *developer's, integrator's, distributor's, or deployer's business; (iv) the substantial likelihood of injury to the*
455 *public; (v) the safety of persons or property; (vi) whether such violation was likely caused by human or*
456 *technical error. If the developer, integrator, distributor, or deployer fails to cure such violation within 45*
457 *days of the receipt of such notice of violation, the Attorney General may proceed with such action.*

458 *I. Nothing in this chapter shall create a private cause of action in favor of any person aggrieved by a*
459 *violation of this chapter.*

460 **2. That the provisions of this act shall become effective on July 1, 2026.**

461 **3. That the provisions of this act shall apply only to a violation committed or a cause of action accruing**
462 **on or after July 1, 2026.**