

LC001407

IN GENERAL ASSEMBLY

RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS --
ARTIFICIAL INTELLIGENCE ACT

Referred To: Senate Artificial Intelligence & Emerging Tech

1 SECTION 1. Title 6 of the General Laws entitled "COMMERCIAL LAW — GENERAL
2 REGULATORY PROVISIONS" is hereby amended by adding thereto the following chapter:

ARTIFICIAL INTELLIGENCE ACT

18 (II) Expanding an applicant, customer or participant pool to increase diversity or redress

1 historic discrimination; or

2 (B) An act or omission by or on behalf of a private club or other establishment not in fact
3 open to the public, as set forth in Title II of the Civil Rights Act of 1964, 42 USC § 2000a(e), as
4 amended from time to time.

5 (2) "Artificial intelligence system" means any machine-based system that, for any explicit
6 or implicit objective, infers from the inputs such system receives how to generate outputs including,
7 but not limited to, content, decisions, predictions or recommendations, that can influence physical
8 or virtual environments.

9 (3) "Consequential decision" means any decision or judgment that has a legal, material or
10 similarly significant effect on a consumer with respect to:

11 (i) Employment, including any such decision or judgment made:

12 (A) Concerning hiring, termination, compensation or promotion; or

13 (B) By way of any automated task allocation that limits, segregates or classifies employees
14 for the purpose of assigning or determining material terms or conditions of employment;

15 (ii) Education or vocational training, including any such decision or judgment made
16 concerning:

17 (A) Assessments;

18 (B) Student cheating or plagiarism detection;

19 (C) Accreditation;

20 (D) Certification;

21 (E) Admissions; or

22 (F) Financial aid or scholarships;

23 (iii) The provision or denial, or terms and conditions, of:

24 (A) Financial lending or credit services;

25 (B) Housing or lodging including, but not limited to, rentals or short-term housing or
26 lodging;

27 (C) Insurance; or

28 (D) Legal services; or

29 (iv) The provision or denial of:

30 (A) Essential government services; or

31 (B) Healthcare services.

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

33 (5) "Deploy" means to use a high-risk artificial intelligence system to make, or as a
34 substantial factor in making, a consequential decision.

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

3 (7) "Developer" means any person doing business in this state that develops, or
4 intentionally and substantially modifies, an artificial intelligence system.

5 (8) "General-purpose artificial intelligence model" means:
6 (i) Any form of artificial intelligence system that:
7 (A) Displays significant generality;
8 (B) Is capable of competently performing a wide range of distinct tasks;
9 (C) Can be integrated into a variety of downstream applications or systems; and
10 (ii) Does not include any artificial intelligence model that is used for development,
11 prototyping and research activities before such artificial intelligence model is released on the
12 market.

13 (9) "High-risk artificial intelligence system" means:
14 (i) Any artificial intelligence system that, when deployed, makes, or is a substantial factor
15 in making, a consequential decision; and
16 (ii) Does not include:
17 (A) Any artificial intelligence system that is intended to:
18 (I) Perform any narrow procedural task; or
19 (II) Detect decision-making patterns, or deviations from decision-making patterns, unless
20 such artificial intelligence system is intended to replace or influence any assessment previously
21 completed by an individual without sufficient human review; or
22 (B) Unless the technology, when deployed, makes, or is a substantial factor in making, a
23 consequential decision:
24 (I) Any anti-fraud technology that does not make use of facial recognition technology;
25 (II) Any artificial intelligence-enabled video game technology;
26 (III) Any anti-malware, anti-virus, calculator, cybersecurity, database, data storage,
27 firewall, Internet domain registration, Internet-website loading, networking, robocall-filtering,
28 spam-filtering, spellchecking, spreadsheet, web-caching, web-hosting or similar technology;
29 (IV) Any technology that performs tasks exclusively related to an entity's internal
30 management affairs including, but not limited to, ordering office supplies or processing payments;
31 or
32 (V) Any technology that communicates with consumers in natural language for the purpose
33 of providing users with information, making referrals or recommendations and answering
34 questions, and is subject to an accepted use policy that prohibits generating content that is

1 discriminatory or harmful;

2 (10) "Integrator" means any person doing business in this state that, with respect to a given

3 high-risk artificial intelligence system:

4 (i) Neither develops nor intentionally and substantially modifies the high-risk artificial

5 intelligence system; and

6 (ii) Integrates the high-risk artificial intelligence system into a product or service such

7 person offers to any other person.

8 (11) "Intentional and substantial modification" means:

9 (i) Any deliberate change made to:

10 (A) An artificial intelligence system that materially increases the risk of algorithmic

11 discrimination; or

12 (B) A general-purpose artificial intelligence model that:

13 (I) Affects compliance of the general-purpose artificial intelligence model;

14 (II) Materially changes the purpose of the general-purpose artificial intelligence model; or

15 (III) Materially increases the risk of algorithmic discrimination; and

16 (ii) Does not include any change made to a high-risk artificial intelligence system, or the

17 performance of a high-risk artificial intelligence system, if:

18 (A) The high-risk artificial intelligence system continues to learn after such high-risk

19 artificial intelligence system is:

20 (I) Offered, sold, leased, licensed, given or otherwise made available to a deployer; or

21 (II) Is deployed; and

22 (B) Such change:

23 (I) Is made to such high-risk artificial intelligence system as a result of any learning

24 described in subsection (11)(ii)(A) of this section;

25 (II) Was predetermined by the deployer, or the third party contracted by the deployer, when

26 such deployer or third party completed the initial impact assessment of such high-risk artificial

27 intelligence system pursuant to § 6-61-4(c); and

28 (III) Is included in the technical documentation for such high-risk artificial intelligence

29 system.

30 (12) "Person" means any individual, association, corporation, limited liability company,

31 partnership, trust or other legal entity.

32 (13) "Red-teaming" means an exercise that is conducted to identify the potential adverse

33 behaviors or outcomes of an artificial intelligence system, how such behaviors or outcomes occur

34 and stress test the safeguards against such behaviors or outcomes.

1 (14) "Substantial factor" means:

2 (i) A factor that alters the outcome of a consequential decision and is generated by an
3 artificial intelligence system; and

4 (ii) Includes, but is not limited to, any use of an artificial intelligence system to generate
5 any content, decision, prediction or recommendation concerning a consumer that is used as a basis
6 to make a consequential decision concerning the consumer. Substantial factor does not include any
7 output produced by an artificial intelligence system where an individual was involved in the data
8 processing that produced such output and such individual meaningfully considered such data as
9 part of such data processing and had the authority to change or influence the output produced by
10 such data processing.

11 (15) "Synthetic digital content" means any digital content including, but not limited to, any
12 audio, image, text or video, that is produced or manipulated by an artificial intelligence system
13 including, but not limited to, a general-purpose artificial intelligence model.

14 (16) "Trade secret" means information, including a formula, pattern, compilation, program,
15 device, method, technique, or process, that:

16 (i) Derives independent economic value, actual or potential, from not being generally
17 known to, and not being readily ascertainable by proper means by, other persons who can obtain
18 economic value from its disclosure or use; and

19 (ii) Is the subject of efforts that are reasonable under the circumstances to maintain its
20 secrecy.

21 **6-61-3. Artificial intelligence developers.**

22 (a) Beginning on October 1, 2026, a developer of a high-risk artificial intelligence system
23 shall use reasonable care to protect consumers from any known or reasonably foreseeable risks of
24 algorithmic discrimination arising from the intended and contracted uses of the high-risk artificial
25 intelligence system. In any enforcement action brought on or after said date by the attorney general
26 pursuant to the provisions of this chapter, there shall be a rebuttable presumption that a developer
27 used reasonable care as required under this section if the developer complied with the provisions
28 of this section or, if the developer enters into a contract with an integrator as set forth in § 6-61-
29 4(b), the developer and integrator complied with the provisions of this section and § 6-61-4.

30 (b) Except as provided in § 6-61-4(c), a developer of a high-risk artificial intelligence
31 system shall, beginning on October 1, 2026, make available to each deployer, or other developer,
32 of the high-risk artificial intelligence system:

33 (1) A general statement describing the reasonably foreseeable uses, and the known harmful
34 or inappropriate uses, of such high-risk artificial intelligence system;

1 (2) Documentation disclosing:

2 (i) High-level summaries of the type of data used to train such high-risk artificial

3 intelligence system;

4 (ii) The known or reasonably foreseeable limitations of such high-risk artificial intelligence

5 system including, but not limited to, the known or reasonably foreseeable risks of algorithmic

6 discrimination arising from the intended uses of such high-risk artificial intelligence system;

7 (iii) The purpose of such high-risk artificial intelligence system;

8 (iv) The intended benefits and uses of such high-risk artificial intelligence system; and

9 (v) All other information necessary to enable such deployer to comply with the provisions

10 of this chapter;

11 (3) Documentation describing:

12 (i) How such high-risk artificial intelligence system was evaluated for performance, and

13 mitigation of algorithmic discrimination, before such high-risk artificial intelligence system was

14 offered, sold, leased, licensed, given or otherwise made available to such deployer;

15 (ii) The data governance measures used to cover the training datasets and the measures

16 used to examine the suitability of data sources, possible biases and appropriate mitigation;

17 (iii) The intended outputs of such high-risk artificial intelligence system;

18 (iv) The measures the developer has taken to mitigate any known or reasonably foreseeable

19 risks of algorithmic discrimination that may arise from deployment of such high-risk artificial

20 intelligence system; and

21 (v) How such high-risk artificial intelligence system should be used, not be used and be

22 monitored by an individual when such high-risk artificial intelligence system is used to make, or

23 as a substantial factor in making, a consequential decision.

24 (4) Any additional documentation that is reasonably necessary to assist a deployer to:

25 (i) Understand the outputs of such high-risk artificial intelligence system; and

26 (ii) Monitor the performance of such high-risk artificial intelligence system for risks of

27 algorithmic discrimination.

28 (c)(1) Except as provided in § 6-61-4(c), any developer that, on or after October 1, 2026,

29 offers, sells, leases, licenses, gives or otherwise makes available to a deployer or another developer

30 a high-risk artificial intelligence system shall, to the extent feasible, make available to the deployers

31 and other developers of such high-risk artificial intelligence system the documentation and

32 information necessary for a deployer, or the third party contracted by a deployer, to complete an

33 impact assessment pursuant to § 6-61-5(c). The developer shall make such documentation and

34 information available through artifacts such as model cards, dataset cards or other impact

1 assessments.

2 (2) A developer that also serves as a deployer for any high-risk artificial intelligence system
3 shall not be required to generate the documentation required by this section unless such high-risk
4 artificial intelligence system is provided to an unaffiliated entity acting as a deployer.

5 (d)(1) Beginning on October 1, 2026, each developer shall make available, in a manner
6 that is clear and readily available on such developer's Internet website or in a public use case
7 inventory, a statement summarizing:

8 (i) The types of high-risk artificial intelligence systems that such developer:
9 (A) Has developed or intentionally and substantially modified; and
10 (B) Currently makes available to a deployer or another developer; and
11 (ii) How such developer manages any known or reasonably foreseeable risks of algorithmic
12 discrimination that may arise from development or intentional and substantial modification of the
13 types of high-risk artificial intelligence systems described in subsection (d)(1)(i)(A) of this section.

14 (2) Each developer shall update the statement described in subsection (b)(1) of this section
15 as necessary to ensure that such statement remains accurate, and not later than ninety (90) days
16 after the developer intentionally and substantially modifies any high-risk artificial intelligence
17 system described in subsection (d)(1)(i) of this section.

18 (e) Beginning on October 1, 2026, a developer of a high-risk artificial intelligence system
19 shall disclose to the attorney general, in a form and manner prescribed by the attorney general, and
20 to all known deployers or other developers of the high-risk artificial intelligence system, any known
21 or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of such
22 high-risk artificial intelligence system. The developer shall make such disclosures without
23 unreasonable delay but in no event later than ninety (90) days after the date on which:

24 (1) The developer discovers, through the developer's ongoing testing and analysis, that the
25 high-risk artificial intelligence system has:

26 (i) Been deployed; and
27 (ii) Caused, or is reasonably likely to have caused, algorithmic discrimination to at least
28 one thousand (1,000) consumers; or

29 (2) The developer receives, from a deployer of the high-risk artificial intelligence system,
30 a credible report disclosing that such high-risk artificial intelligence system has:

31 (i) Been deployed; and
32 (ii) Caused algorithmic discrimination to at least one thousand (1,000) consumers.

33 (f) The provisions of subsections (b) through (e), inclusive, of this section shall not be
34 construed to require a developer to disclose any information:

1 (1) That is a trade secret or otherwise protected from disclosure under state or federal law;
2 or
3 (2) The disclosure of which would present a security risk to the developer.
4 (g) Beginning on October 1, 2026, the attorney general may require that a developer
5 disclose to the attorney general, as part of an investigation conducted by the attorney general and
6 in a form and manner prescribed by the attorney general, the general statement or documentation
7 described in subsection (b) of this section. The attorney general may evaluate such general
8 statement or documentation to ensure compliance with the provisions of this section. In disclosing
9 such general statement or documentation to the attorney general pursuant to this subsection, the
10 developer may designate such general statement or documentation as including any information
11 that is exempt from disclosure under subsection (f) of this section or the provisions of title 38
12 ("access to public records"). To the extent such general statement or documentation includes such
13 information, such general statement or documentation shall be exempt from disclosure pursuant to
14 the provisions of this chapter or title 38. To the extent any information contained in such general
15 statement or documentation is subject to the attorney-client privilege or work product protection,
16 such disclosure shall not constitute a waiver of such privilege or protection.

17 **6-61-4. High-risk artificial intelligence system.**

18 (a) Beginning on October 1, 2026, if an integrator integrates a high-risk artificial
19 intelligence system into a product or service the integrator offers to any other person, such
20 integrator shall use reasonable care to protect consumers from any known or reasonably foreseeable
21 risks of algorithmic discrimination arising from the intended and contracted uses of such integrated
22 high-risk artificial intelligence system. In any enforcement action brought on or after said date by
23 the attorney general pursuant to the provisions of this chapter, there shall be a rebuttable
24 presumption that the integrator used reasonable care as required under this section if the integrator
25 complied with the provisions of this chapter.

26 (b) Beginning on October 1, 2026, no integrator shall integrate a high-risk artificial
27 intelligence system into a product or service the integrator offers to any other person unless the
28 integrator has entered into a contract with the developer of the high-risk artificial intelligence
29 system. The contract shall be binding and clearly set forth the duties of the developer and integrator
30 with respect to the integrated high-risk artificial intelligence system including, but not limited to,
31 whether the developer or integrator shall be responsible for performing the developer's duties of §
32 6-61-3(b) and (c).

33 (c) The provisions of § 6-61-3(b) and (c) shall not apply to a developer of an integrated
34 high-risk artificial intelligence system if, at all times while the integrated high-risk artificial

intelligence system is integrated into a product or service an integrator offers to any other person.
the developer has entered into a contract with the integrator in which such integrator has agreed to
assume the developer's duties under § 6-61-3(b) and (c).

(d)(1) Beginning on October 1, 2026, each integrator shall make available, in a manner that
is clear and readily available on such integrator's Internet website or in a public use case inventory,
a statement summarizing:

(i) The types of high-risk artificial intelligence systems that such integrator has integrated
into products or services such integrator currently offers to any other person; and

(ii) How such integrator manages any known or reasonably foreseeable risks of algorithmic
discrimination that may arise from the types of high-risk artificial intelligence systems described
in this chapter.

(2) Each integrator shall update the statement described in subsection (d)(1) of this section:

(i) As necessary to ensure that such statement remains accurate; and

(ii) Not later than ninety (90) days after any intentional and substantial modification is
made to any high-risk artificial intelligence system described in subsection (d)(1) of this section.

(e) The provisions of subsections (b) through (d), inclusive, of this section shall not be
construed to require a developer or integrator to disclose any information:

(1) That is a trade secret or otherwise protected from disclosure under state or federal law;
or

(2) The disclosure of which would present a security risk to the developer or integrator.

(f) Beginning on October 1, 2026, the attorney general may require that a developer
disclose to the attorney general, as part of an investigation conducted by the attorney general and
in a form and manner prescribed by the attorney general, the general statement or documentation
described in subsection (b) of this section. The attorney general may evaluate such general
statement or documentation to ensure compliance with the provisions of this section. In disclosing
such general statement or documentation to the attorney general pursuant to this subsection, the
developer may designate such general statement or documentation as including any information
that is exempt from disclosure under subsection (e) of this section or the provisions of title 38
("access to public records"). To the extent such general statement or documentation includes such
information, such general statement or documentation shall be exempt from disclosure pursuant to
the provisions of this chapter or title 38. To the extent any information contained in such general
statement or documentation is subject to the attorney-client privilege or work product protection,
such disclosure shall not constitute a waiver of such privilege or protection.

6-61-5. Reasonable care to protect from foreseeable risks.

1 (a) Beginning on October 1, 2026, each deployer of a high-risk artificial intelligence system
2 shall use reasonable care to protect consumers from any known or reasonably foreseeable risks of
3 algorithmic discrimination. In any enforcement action brought on or after said date by the attorney
4 general pursuant to the provisions of this chapter, there shall be a rebuttable presumption that a
5 section of a high-risk artificial intelligence system used reasonable care as required under this
6 subsection if the deployer complied with the provisions of this chapter.

7 (b)(1) Beginning on October 1, 2026, and except as provided in subsection (g) of this
8 section, each deployer of a high-risk artificial intelligence system shall implement and maintain a
9 risk management policy and program to govern such deployer's deployment of the high-risk
10 artificial intelligence system. The risk management policy and program shall specify and
11 incorporate the principles, processes and personnel that the deployer shall use to identify, document
12 and mitigate any known or reasonably foreseeable risks of algorithmic discrimination. The risk
13 management policy shall be the product of an iterative process, the risk management program shall
14 be an iterative process and both the risk management policy and program shall be planned,
15 implemented and regularly and systematically reviewed and updated over the lifecycle of the high-
16 risk artificial intelligence system. Each risk management policy and program implemented and
17 maintained pursuant to this subsection shall be reasonable, considering:

18 (i) The guidance and standards set forth in the latest version of:

19 (A) The "Artificial Intelligence Risk Management Framework" published by the National
20 Institute of Standards and Technology;

21 (B) ISO or IEC 42001 of the International Organization for Standardization; or

22 (C) A nationally or internationally recognized risk management framework for artificial
23 intelligence systems, other than the guidance and standards specified in this subsection, that
24 imposes requirements that are substantially equivalent to, and at least as stringent as, the
25 requirements set forth in this section for risk management policies and programs;

26 (ii) The size and complexity of the deployer;

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

30 (iv) The sensitivity and volume of data processed in connection with the high-risk artificial
31 intelligence systems deployed by the deployer.

32 (2) A risk management policy and program implemented and maintained pursuant to
33 subsection (b)(1) of this section may cover multiple high-risk artificial intelligence systems
34 deployed by the deployer.

1 (c)(1) Except as provided in subsections (c)(3), (c)(4) and (g) of this section:

2 (i) A deployer that deploys a high-risk artificial intelligence system on or after October 1,

3 2026, or a third party contracted by the deployer, shall complete an impact assessment of the high-

4 risk artificial intelligence system; and

5 (ii) Beginning on October 1, 2026, a deployer, or a third party contracted by the deployer,

6 shall complete an impact assessment of a deployed high-risk artificial intelligence system:

7 (A) At least annually; and

8 (B) Not later than ninety (90) days after an intentional and substantial modification to such

9 high-risk artificial intelligence system is made available.

10 (2)(i) Each impact assessment completed pursuant to this subsection shall include, at a

11 minimum and to the extent reasonably known by, or available to, the deployer:

12 (A) A statement by the deployer disclosing the purpose, intended use cases and deployment

13 context of, and benefits afforded by, the high-risk artificial intelligence system;

14 (B) An analysis of whether the deployment of the high-risk artificial intelligence system

15 poses any known or reasonably foreseeable risks of algorithmic discrimination and, if so, the nature

16 of such algorithmic discrimination and the steps that have been taken to mitigate such risks;

17 (C) A description of:

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

19 and

20 (II) The outputs such high-risk artificial intelligence system produces;

21 (D) If the deployer used data to customize the high-risk artificial intelligence system, an

22 overview of the categories of data the deployer used to customize such high-risk artificial

23 intelligence system;

24 (E) Any metrics used to evaluate the performance and known limitations of the high-risk

25 artificial intelligence system;

26 (F) A description of any transparency measures taken concerning the high-risk artificial

27 intelligence system including, but not limited to, any measures taken to disclose to a consumer that

28 such high-risk artificial intelligence system is in use when such high-risk artificial intelligence

29 system is in use; and

30 (G) A description of the post-deployment monitoring and user safeguards provided

31 concerning such high-risk artificial intelligence system including, but not limited to, the oversight,

32 use and learning process established by the deployer to address issues arising from deployment of

33 such high-risk artificial intelligence system.

34 (ii) In addition to the statement, analysis, descriptions, overview and metrics required under

1 subsection (c)(2) of this section, an impact assessment completed pursuant to this subsection
2 following an intentional and substantial modification made to a high-risk artificial intelligence
3 system on or after October 1, 2026, shall include a statement disclosing the extent to which the
4 high-risk artificial intelligence system was used in a manner that was consistent with, or varied
5 from, the developer's intended uses of such high-risk artificial intelligence system.

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

8 (iv) If a deployer, or a third party contracted by the deployer, completes an impact
9 assessment for the purpose of complying with another applicable law or regulation, such impact
10 assessment shall be deemed to satisfy the requirements established in this subsection if such impact
11 assessment is reasonably similar in scope and effect to the impact assessment that would otherwise
12 be completed pursuant to this subsection.

13 (v) A deployer shall maintain the most recently completed impact assessment of a high-
14 risk artificial intelligence system as required under this subsection, all records concerning each such
15 impact assessment and all prior impact assessments, if any, for a period of at least three (3) years
16 following the final deployment of the high-risk artificial intelligence system.

17 (d) Except as provided in subsection (g) of this section, a deployer, or a third party
18 contracted by the deployer, shall review, not later than October 1, 2026, and at least annually
19 thereafter, the deployment of each high-risk artificial intelligence system deployed by the deployer
20 to ensure that such high-risk artificial intelligence system is not causing algorithmic discrimination.

21 (e)(1) Beginning on October 1, 2026, and before a deployer deploys a high-risk artificial
22 intelligence system to make, or be a substantial factor in making, a consequential decision
23 concerning a consumer, the deployer shall:

24 (i) Notify the consumer that the deployer has deployed a high-risk artificial intelligence
25 system to make, or be a substantial factor in making, such consequential decision; and

26 (ii) Provide to the consumer:

27 (A) A statement disclosing:

28 (I) The purpose of such high-risk artificial intelligence system; and

29 (II) The nature of such consequential decision;

30 (B) The right to opt-out of any automated decision-making based on the consumer's
31 personal data;

32 (C) Contact information for such deployer;

33 (D) A description, in plain language, of such high-risk artificial intelligence system; and

34 (E) Instructions on how to access the statement made available pursuant to subsection (f)

1 of this section.

2 (2) Beginning on October 1, 2026, a deployer that has deployed a high-risk artificial
3 intelligence system to make, or as a substantial factor in making, a consequential decision
4 concerning a consumer shall, if such consequential decision is adverse to the consumer, provide to
5 such consumer:

6 (i) A statement disclosing the principal reason or reasons for such adverse consequential
7 decision including, but not limited to:

8 (A) The degree to which, and manner in which, the high-risk artificial intelligence system
9 contributed to such adverse consequential decision;

10 (B) The type of data that were processed by such high-risk artificial intelligence system in
11 making such adverse consequential decision; and

12 (C) The source of the data described in this subsection;

13 (ii) An opportunity to:

14 (A) Examine the personal data that the high-risk artificial intelligence system processed in
15 making, or as a substantial factor in making, such adverse consequential decision; and

16 (B) Correct any incorrect personal data described in this subsection; and

17 (3)(i) Except as provided in this subsection, an opportunity to appeal such adverse
18 consequential decision if such adverse consequential decision is based upon inaccurate personal
19 data, taking into account both the nature of such personal data and the purpose for which such
20 personal data was processed. Such appeal shall, if technically feasible, allow for human review.

21 (ii) No deployer shall be required to provide an opportunity to appeal pursuant to
22 subsection (e)(3)(i) of this section in any instance in which providing such opportunity to appeal is
23 not in the best interest of the consumer including, but not limited to, in any instance in which any
24 delay might pose a risk to the life or safety of the consumer.

25 (iii) The deployer shall provide the notice, statements, information, description and
26 instructions required under the provisions of this subsection:

27 (A) Directly to the consumer;

28 (B) In plain language;

29 (C) In all languages in which such deployer, in the ordinary course of such deployer's
30 business, provides contracts, disclaimers, sale announcements and other information to consumers;
31 and

32 (D) In a format that is accessible to consumers with disabilities.

33 (f)(1) Beginning on October 1, 2026, and except as provided in subsection (g) of this
34 section, each deployer shall make available, in a manner that is clear and readily available on such

1 deployer's Internet website, a statement summarizing:

2 (i) The types of high-risk artificial intelligence systems that are currently deployed by such

3 deployer;

4 (ii) How such deployer manages any known or reasonably foreseeable risks of algorithmic

5 discrimination that may arise from deployment of each high-risk artificial intelligence system

6 described in this subsection; and

7 (iii) In detail, the nature, source and extent of the information collected and used by such

8 deployer.

9 (2) Each deployer shall periodically update the statement described in subsection(f)(1) of

10 this section.

11 (g) The provisions of subsections (b) through (d), inclusive, of this section and subsection

12 (f) of this section shall not apply to a deployer if, at the time the deployer deploys a high-risk

13 artificial intelligence system and at all times while the high-risk artificial intelligence system is

14 deployed:

15 (1) The deployer:

16 (i) Has entered into a contract with the developer in which the developer has agreed to

17 assume the deployer's duties under subsections (b) through (d), inclusive, of this section and

18 subsection (f) of this section and

19 (ii) Does not exclusively use such deployer's own data to train such high-risk artificial

20 intelligence system;

21 (2) Such high-risk artificial intelligence system:

22 (i) Is used for the intended uses that are disclosed to such deployer; and

23 (ii) Continues learning based on a broad range of data sources and not solely based on the

24 deployer's own data; and

25 (3) Such deployer makes available to consumers any impact assessment that:

26 (i) The developer of such high-risk artificial intelligence system has completed and

27 provided to such deployer; and

28 (ii) Includes information that is substantially similar to the information included in the

29 statement, analysis, descriptions, overview and metrics required pursuant to the provisions of this

30 section.

31 (h) If a deployer deploys a high-risk artificial intelligence system on or after October 1,

32 2026, and subsequently discovers that the high-risk artificial intelligence system has caused

33 algorithmic discrimination to at least one thousand (1,000) consumers, the deployer shall send to

34 the attorney general, in a form and manner prescribed by the attorney general, a notice disclosing

1 such discovery. The deployer shall send such notice to the attorney general without unreasonable
2 delay but in no event later than ninety (90) days after the date on which the deployer discovered
3 such algorithmic discrimination.

4 (i) Nothing in subsections (b) through (h), inclusive, of this section shall be construed to
5 require a deployer to disclose any information that is a trade secret or otherwise protected from
6 disclosure under state or federal law. If a deployer withholds any information from a consumer
7 under this subsection, the deployer shall send notice to the consumer disclosing:

8 (A) That the deployer is withholding such information from such consumer; and

9 (B) The basis for the deployer's decision to withhold such information from such consumer.

10 (j) Beginning on October 1, 2026, the attorney general may require that a deployer, or a
11 third party contracted by the deployer as set forth in subsection (c) of this section, as applicable,
12 disclose to the attorney general, as part of an investigation conducted by the attorney general, not
13 later than ninety (90) days after a request by the attorney general and in a form and manner
14 prescribed by the attorney general, the risk management policy implemented pursuant to subsection
15 (b) of this section, impact assessment completed pursuant to subsection (c) of this section or records
16 maintained pursuant to the provisions of subsection (c) of this section. The attorney general may
17 evaluate such risk management policy, impact assessment or records to ensure compliance with the
18 provisions of this section. In disclosing such risk management policy, impact assessment or records
19 to the attorney general pursuant to this subsection, the deployer or third-party contractor, as
20 applicable, may designate such risk management policy, impact assessment or records as including
21 any information that is exempt from disclosure under subsection (i) of this section or chapter 2 of
22 title 38 ("access to public records"). To the extent such risk management policy, impact assessment
23 or records include such information, such risk management policy, impact assessment or records
24 shall be exempt from disclosure pursuant to the provisions of this chapter or title 38. To the extent
25 any information contained in such risk management policy, impact assessment or record is subject
26 to the attorney-client privilege or work product protection, such disclosure shall not constitute a
27 waiver of such privilege or protection.

28 **6-61-6. Technical documentation.**

29 (a) Beginning on October 1, 2026, each developer of a general-purpose artificial
30 intelligence model shall, except as provided in subsection (b) of this section:

31 (1)(i) Create and maintain technical documentation for the general-purpose artificial
32 intelligence model, which technical documentation shall:

33 (A) Include the training and testing processes for such general-purpose artificial
34 intelligence model;

1 (B) Include at least the following information, as appropriate, considering the size and risk
2 profile of such general-purpose artificial intelligence model:

3 (I) The tasks such general-purpose artificial intelligence model is intended to perform;

4 (II) The type and nature of artificial intelligence systems in which such general-purpose
5 artificial intelligence model is intended to be integrated;

6 (III) Acceptable use policies for such general-purpose artificial intelligence model;

7 (IV) The date such general-purpose artificial intelligence model is released;

8 (V) The methods by which such general-purpose artificial intelligence model is distributed;
9 and

10 (VI) The modality and format of inputs and outputs for such general-purpose artificial
11 intelligence model.

12 (C) Include a description of the data that were used for purposes of training, testing and
13 validation of such general-purpose artificial intelligence model, which description shall be
14 appropriate considering the size and risk profile of such general-purpose artificial intelligence
15 model and include, at a minimum, a description of the following:

16 (I) The type and provenance of such data;

17 (II) Curation methodologies used for such data;

18 (III) How such data were obtained and selected;

19 (IV) All measures used to identify unsuitable data sources; and

20 (V) Where applicable, methods used to detect identifiable biases;

21 (D) Be reviewed and revised at least annually or more frequently as necessary to maintain
22 the accuracy of such technical documentation;

23 (E) Establish, implement and maintain a policy to comply with federal and state copyright
24 laws;

25 (F) Create, implement, maintain and make available to persons that intend to integrate such
26 general-purpose artificial intelligence model into such persons' artificial intelligence systems
27 documentation and information that:

28 (2) Enables such persons to:

29 (i) Understand the capabilities and limitations of such general-purpose artificial
30 intelligence model; and

31 (ii) Comply with such persons' obligations under this chapter;

32 (3) Discloses, at a minimum:

33 (i) The technical means required for such general-purpose artificial intelligence model to
34 be integrated into such persons' artificial intelligence systems;

1 (ii) The information listed in subsection (a)(1) of this section; and
2 (iii) The description required under subsection (a)(1)(i)(C) of this section; and
3 (4) Except as provided in subsection (b) of this section, is reviewed and revised at least
4 annually or more frequently as necessary to maintain the accuracy of such documentation and
5 information.

6 (b)(1) The provisions of subsection (a)(1) and (a)(2)(c) of this section shall not apply to a
7 developer that develops, or intentionally and substantially modifies, a general-purpose artificial
8 intelligence model on or after October 1, 2026, if:

9 (i) The developer releases such general-purpose artificial intelligence model under a free
10 and open-source license that allows for:

11 (A) Access to, and modification, distribution and usage of, such general-purpose artificial
12 intelligence model; and

13 (B) The parameters of such general-purpose artificial intelligence model to be made
14 publicly available as set forth in this subsection; and

15 (ii) Unless such general-purpose artificial intelligence model is deployed as a high-risk
16 artificial intelligence system, the parameters of such general-purpose artificial intelligence model
17 including, but not limited to, the weights and information concerning the model architecture and
18 model usage for such general-purpose artificial intelligence model, are made publicly available; or

19 (iii) The general-purpose artificial intelligence model is:

20 (A) Not offered for sale in the market;

21 (B) Not intended to interact with consumers; and

22 (C) Solely utilized:

23 (I) For an entity's internal purposes; or

24 (II) Under an agreement between multiple entities for such entities' internal purposes.

25 (3) The provisions of this section shall not apply to a developer that develops, or
26 intentionally and substantially modifies, a general-purpose artificial intelligence model on or after
27 October 1, 2026, if such general purpose artificial intelligence model performs tasks exclusively
28 related to an entity's internal management affairs including, but not limited to, ordering office
29 supplies or processing payments.

30 (4) A developer that takes any action under an exemption established in this subsection
31 shall bear the burden of demonstrating that such action qualifies for such exemption.

32 (5) A developer that is exempt under this subsection shall establish and maintain an
33 artificial intelligence risk management framework, which framework shall:

34 (i) Be the product of an iterative process and ongoing efforts; and

1 (ii) Include, at a minimum:

2 (A) An internal governance function;

3 (B) A map function that shall establish the context to frame risks;

4 (C) A risk management function; and

5 (D) A function to measure identified risks by assessing, analyzing and tracking such risks.

6 (c) Nothing in subsection (a) of this section shall be construed to require a developer to

7 disclose any information that is a trade secret or otherwise protected from disclosure under state or

8 federal law.

9 (d) Beginning on October 1, 2026, the attorney general may require that a developer

10 disclose to the attorney general, as part of an investigation conducted by the attorney general, not

11 later than ninety (90) days after a request by the attorney general and in a form and manner

12 prescribed by the attorney general, any documentation maintained pursuant to this section. The

13 attorney general may evaluate such documentation to ensure compliance with the provisions of this

14 section. In disclosing any documentation to the attorney general pursuant to this subsection, the

15 developer may designate such documentation as including any information that is exempt from

16 disclosure under subsection (c) of this section or chapter 2 of title 38 ("access to public records").

17 To the extent such documentation includes such information, such documentation shall be exempt

18 from disclosure under the provision of this chapter or chapter 2 of title 38. To the extent any

19 information contained in such documentation is subject to the attorney-client privilege or work

20 product protection, such disclosure shall not constitute a waiver of such privilege or protection.

21 **6-61-7. Artificial intelligence system designation.**

22 (a) Beginning on October 1, 2026, and except as provided in subsections (b) and (c) of this

23 section, the developer of an artificial intelligence system including, but not limited to, a general-

24 purpose artificial intelligence model, that generates or manipulates synthetic digital content shall:

25 (1) Ensure that the outputs of such artificial intelligence system are marked and detectable

26 as synthetic digital content, and that such outputs are so marked and detectable;

27 (i) Not later than the time that consumers who did not create such outputs first interact

28 with, or are exposed to, such outputs; and

29 (ii) In a manner that:

30 (A) Is detectable by consumers; and

31 (B) Complies with any applicable accessibility requirements; and

32 (2) As far as technically feasible and in a manner that is consistent with any nationally or

33 internationally recognized technical standards, ensure that such developer's technical solutions are

34 effective, interoperable, robust and reliable, considering:

1 (i) The specificities and limitations of different types of synthetic digital content;
2 (ii) The implementation costs; and
3 (iii) The generally acknowledged state of the art.
4 (b) If the synthetic digital content described in subsection (a) of this section is in an audio,
5 image or video format, and such synthetic digital content forms part of an evidently artistic,
6 creative, satirical, fictional analogous work or program, the disclosure required under said
7 subsection shall be limited to a disclosure that does not hinder the display or enjoyment of such
8 work or program.
9 (c) The provisions of subsection (a) of this section shall not apply to:
10 (1) Any synthetic digital content that:
11 (i) Consists exclusively of text;
12 (ii) Is published to inform the public on any matter of public interest; or
13 (iii) Is unlikely to mislead a reasonable person consuming such synthetic digital content;
14 or
15 (2) To the extent that any artificial intelligence system described in subsection (a) of this
16 section:
17 (i) Performs an assistive function for standard editing;
18 (ii) Does not substantially alter the input data provided by the developer or the semantics
19 thereof; or
20 (iii) Is used to detect, prevent a violation of the provisions of this chapter or other laws or
21 regulations.
22 **6-61-8. Compliance with other laws.**
23 (a) Nothing in this chapter shall be construed to restrict a developer's, integrator's,
24 deployer's or other person's ability to:
25 (1) Comply with federal, state or municipal law;
26 (2) Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or
27 summons by a federal, state, municipal or other governmental authority;
28 (3) Cooperate with a law enforcement agency concerning conduct or activity that the
29 developer, integrator, deployer or other person reasonably and in good faith believes may violate
30 federal, state or municipal law;
31 (4) Investigate, establish, exercise, prepare for or defend a legal claim;
32 (5) Take immediate steps to protect an interest that is essential for the life or physical safety
33 of a consumer or another individual;
34 (6)(i) By any means other than facial recognition technology, prevent, detect, protect

1 against or respond to:

2 (A) A security incident;

3 (B) A malicious or deceptive activity; or

4 (C) Identity theft, fraud, harassment or any other illegal activity.

5 (ii) Investigate, report or prosecute the persons responsible for any action described in a

6 security incident; or

7 (iii) Preserve the integrity or security of systems;

8 (7) Engage in public or peer-reviewed scientific or statistical research in the public interest

9 that:

10 (i) Adheres to all other applicable ethics and privacy laws; and

11 (ii) Is conducted in accordance with:

12 (A) The provisions of 45 CFR Part 46, as amended from time to time; or

13 (B) Relevant requirements established by the federal Food and Drug Administration;

14 (8) Conduct research, testing, development and integration activities regarding an artificial

15 intelligence system or model, other than testing conducted under real world conditions, before such

16 artificial intelligence system or model is placed on the market, deployed or put into service, as

17 applicable;

18 (9) Effectuate a product recall;

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

20 (11) Assist another developer, integrator, deployer or person with any of the obligations

21 imposed pursuant to the provisions of this chapter.

22 (b) The obligations imposed on developers, integrators, deployers or other persons under

23 this chapter shall not apply where compliance by the developer, integrator, deployer or other person

24 with said provisions of this chapter shall violate an evidentiary privilege under the laws of this state.

25 (c) Nothing in this chapter shall be construed to impose any obligation on a developer,

26 integrator, deployer or other person that adversely affects the rights or freedoms of any person

27 including, but not limited to, the rights of any person to freedom of speech or freedom of the press

28 guaranteed in:

29 (1) The First Amendment to the United States Constitution; and

30 (2) The Rhode Island Constitution, Article 1, § 21.

31 (d) Nothing in this chapter shall be construed to apply to any developer, integrator,

32 deployer, or other person:

33 (1) Insofar as such developer, integrator, deployer or other person develops, integrates,

34 deploys, puts into service or intentionally and substantially modifies, as applicable, a high-risk

1 artificial intelligence system:

2 (i) That has been approved, authorized, certified, cleared, developed, integrated or granted

3 by:

4 (A) A federal agency, such as the federal Food and Drug Administration or the Federal

5 Aviation Administration, acting within the scope of such federal agency's authority; or

6 (B) A regulated entity subject to supervision and regulation by the Federal Housing Finance

7 Agency; or

8 (ii) In compliance with standards that are:

9 (A) Established by:

10 (I) Any federal agency including, but not limited to, the federal Office of the National

11 Coordinator for Health Information Technology; or

12 (II) A regulated entity subject to supervision and regulation by the Federal Housing Finance

13 Agency; and

14 (B) Substantially equivalent to, and at least as stringent as, the standards established in this

15 chapter;

16 (2) Conducting research to support an application:

17 (i) For approval or certification from any federal agency including, but not limited to, the

18 Federal Aviation Administration, the Federal Communications Commission, or the federal Food

19 and Drug Administration; or

20 (ii) That is otherwise subject to review by any federal agency;

21 (3) Performing work under, or in connection with, a contract with the United States

22 Department of Commerce, the United States Department of Defense, or the National Aeronautics

23 and Space Administration, unless such developer, integrator, deployer or other person is performing

24 such work on a high-risk artificial intelligence system that is used to make, or as a substantial factor

25 in making, a decision concerning employment or housing; or

26 (4) That is a covered entity within the meaning of the Health Insurance Portability and

27 Accountability Act of 1996, Pub. L. 104-191, and the regulations promulgated thereunder, as both

28 may be amended from time to time, and providing healthcare recommendations that:

29 (i) Are generated by an artificial intelligence system;

30 (ii) Require a healthcare provider to take action to implement such recommendations; and

31 (iii) Are not considered to be high risk.

32 (e) Nothing in this chapter shall be construed to apply to any artificial intelligence system

33 that is acquired by or for the federal government or any federal agency or department including,

34 but not limited to, the United States Department of Commerce, the United States Department of

1 Defense, or the National Aeronautics and Space Administration, unless such artificial intelligence
2 system is a high-risk artificial intelligence system that is used to make, or as a substantial factor in
3 making, a decision concerning employment or housing.

4 (f) Any insurer, subject to the provisions of title 27, fraternal benefit society, within the
5 meaning of § 27-25-1, or health carrier, as defined in § 27-18.6-2, shall be deemed to be in full
6 compliance with the provisions of this chapter if such insurer, fraternal benefit society or health
7 carrier has implemented and maintains a written artificial intelligence systems program in
8 accordance with all requirements established by the insurance commissioner defined in § 27-2.4-
9 2.

10 (g)(1) Any financial institution, out-of-state financial institution, Rhode Island credit
11 union, federal credit union or out-of-state credit union, or any branch or subsidiary thereof, shall
12 be deemed to be in full compliance with the provisions of this chapter if such financial institution,
13 out-of-state financial institution, Rhode Island credit union, federal credit union, out-of-state credit
14 union, branch or subsidiary is subject to examination by any state or federal prudential regulator
15 under any published guidance or regulations that apply to the use of high-risk artificial intelligence
16 systems and such guidance or regulations:

17 (i) Impose requirements that are substantially equivalent to, and at least as stringent as, the
18 requirements set forth in this chapter; and

19 (ii) At a minimum, require such financial institution, out-of-state financial institution,
20 Rhode Island credit union, federal credit union, out-of-state credit union, branch or subsidiary to:

21 (A) Regularly audit such financial institution's, out-of-state financial institution's, Rhode
22 Island credit union's, federal credit union's, out-of-state credit union's, branch 's or subsidiary's use
23 of high-risk artificial intelligence systems for compliance with state and federal anti-discrimination
24 laws and regulations applicable to such financial institution, out-of-state financial institution,
25 Rhode Island credit union, federal credit union, out-of-state credit union, branch or subsidiary; and

26 (B) Mitigate any algorithmic discrimination caused by the use of a high-risk artificial
27 intelligence system or any risk of algorithmic discrimination that is reasonably foreseeable as a
28 result of the use of a high-risk artificial intelligence system.

29 (2) For the purposes of this section, "branch", "financial institution", "Rhode Island credit
30 union", and "federal credit union" have the same meaning as provided in § 19-1-1.

31 (3) For the purposes of this section, "out-of-state financial institution" means a financial
32 institution whose principal office is located in any other state.

33 (4) For the purposes of this section, "out-of-state credit union" means a credit union whose
34 principal office is located in any other state.

1 (h) If a developer, integrator, deployer or other person engages in any action pursuant to
2 an exemption set forth in subsections (a) through (g), inclusive, of this section, the developer,
3 integrator, deployer or other person bears the burden of demonstrating that such action qualifies for
4 such exemption.

5 **6-61-9. Enforcement.**

6 (a) The attorney general shall have exclusive authority to enforce the provisions of this
7 chapter.

8 (b) Except as provided in subsection (f) of this section, during the period beginning on
9 October 1, 2026, and ending on September 30, 2027, the attorney general shall, prior to initiating
10 any action for a violation of any provision of this chapter, issue a notice of violation to the
11 developer, integrator, deployer, or other person if the attorney general determines that it is possible
12 to cure such violation. If the developer, integrator, deployer or other person fails to cure such
13 violation not later than sixty (60) days after receipt of the notice of violation, the attorney general
14 may bring an action pursuant to this chapter.

15 (c) Except as provided in subsection (f) of this section, beginning on October 1, 2027, the
16 attorney general may, in determining whether to grant a developer, integrator, deployer or other
17 person the opportunity to cure a violation described in subsection (b) of this section, consider:

18 (1) The number of violations;

19 (2) The size and complexity of the developer, integrator, deployer or other person;

20 (3) The nature and extent of the developer's, integrator's, deployer's or other person's
21 business;

22 (4) The substantial likelihood of injury to the public;

23 (5) The safety of persons or property; and

24 (6) Whether such violation was likely caused by human or technical error.

25 (d) Nothing in this chapter shall be construed as providing the basis for a private right of
26 action for violations of this chapter.

27 (e) Except as provided in subsections (a) through (d), inclusive, of this section and
28 subsection (f) of this section, a violation of the requirements established in this chapter shall
29 constitute an unfair trade practice for purposes of § 6-13.1-5 and shall be enforced solely by the
30 attorney general.

31 (f)(1) In any action commenced by the attorney general for any violation of this chapter, it
32 shall be an affirmative defense that the developer, integrator, deployer, or other person:

33 (i) Discovered a violation of any provision of this chapter through red-teaming;

34 (ii) Not later than sixty (60) days after discovering the violation as set forth in subsection

1 (f)(1)(i) of this section:

2 (A) Cures such violation; and

3 (B) Provides to the attorney general, in a form and manner prescribed by the attorney

4 general, notice that such violation has been cured and evidence that any harm caused by such

5 violation has been mitigated; and

6 (iii) Is otherwise in compliance with the latest version of:

7 (A) The "Artificial Intelligence Risk Management Framework" published by the National

8 Institute of Standards and Technology;

9 (B) ISO or IEC 42001 of the International Organization for Standardization;

10 (C) A nationally or internationally recognized risk management framework for artificial

11 intelligence systems, other than the risk management frameworks specified in this subsection, that

12 imposes requirements that are substantially equivalent to, and at least as stringent as, the

13 requirements set forth in this chapter; or

14 (D) Any risk management framework for artificial intelligence systems that is substantially

15 equivalent to, and at least as stringent as, the risk management frameworks described in this

16 subsection.

17 (2) The developer, integrator, deployer or other person bears the burden of demonstrating

18 to the attorney general that the requirements established in subsection (f)(1) of this section have

19 been satisfied.

20 (3) Nothing in this this chapter including, but not limited to, the enforcement authority

21 granted to the attorney general under this section, shall be construed to preempt or otherwise affect

22 any right, claim, remedy, presumption or defense available at law or in equity. Any rebuttable

23 presumption or affirmative defense established under this chapter shall apply only to an

24 enforcement action brought by the attorney general pursuant to this section and shall not apply to

25 any right, claim, remedy, presumption, or defense available at law or in equity.

26 SECTION 2. This act shall take effect on October 1, 2025

=====
LC001407
=====

EXPLANATION
BY THE LEGISLATIVE COUNCIL
OF
A N A C T
RELATING TO COMMERCIAL LAW -- GENERAL REGULATORY PROVISIONS --
ARTIFICIAL INTELLIGENCE ACT

1 This act would establish regulations to ensure the ethical development, integration, and
2 deployment of high-risk Artificial Intelligence (AI) systems, particularly those influencing
3 consequential decisions in areas like employment, education, lending, housing, healthcare, and
4 legal services. It would require developers, integrators, and deployers to use reasonable care to
5 prevent algorithmic discrimination, implement risk management policies, conduct regular impact
6 assessments, and provide transparency regarding the use of AI systems. The act also would require
7 developers to disclose known risks to the attorney general and affected parties, while deployers are
8 required to notify consumers when AI is used in decision-making and offer avenues to appeal
9 adverse outcomes. The act would further mandates that synthetic digital content generated by AI
10 be clearly marked, with exceptions for informational content. Additionally, this act would provide
11 exemptions for AI systems governed by equivalent federal standards, used for internal business
12 purposes, or developed for specific federal agencies. The attorney general would hold exclusive
13 enforcement authority, with a focus on encouraging compliance before pursuing legal action.

14 This act would take effect on October 1, 2025

=====
LC001407
=====