

118TH CONGRESS
1ST SESSION

S. 3312

To provide a framework for artificial intelligence innovation and accountability, and for other purposes.

IN THE SENATE OF THE UNITED STATES

NOVEMBER 15, 2023

Mr. THUNE (for himself, Ms. KLOBUCHAR, Mr. WICKER, Mr. HICKENLOOPER, Mr. LUJÁN, and Mrs. CAPITO) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To provide a framework for artificial intelligence innovation and accountability, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Artificial Intelligence
5 Research, Innovation, and Accountability Act of 2023”.

6 **SEC. 2. TABLE OF CONTENTS.**

7 The table of contents for this Act is as follows:

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

TITLE I—ARTIFICIAL INTELLIGENCE RESEARCH AND
INNOVATION

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

TITLE II—ARTIFICIAL INTELLIGENCE ACCOUNTABILITY

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

1 **TITLE I—ARTIFICIAL INTEL-** 2 **LIGENCE RESEARCH AND IN-** 3 **NOVATION**

4 **SEC. 101. OPEN DATA POLICY AMENDMENTS.**

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

7 (1) in paragraph (22)—

8 (A) by inserting “or data model” after “a
9 data asset”; and

10 (B) by striking “and” at the end;

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

13 (3) by adding at the end the following:

14 “(24) the term ‘data model’ means a mathe-
15 matical, economic, or statistical representation of a

1 system or process used to assist in making calcula-
2 tions and predictions, including through the use of
3 algorithms, computer programs, or artificial intel-
4 ligence systems; and

5 “(25) the term ‘artificial intelligence system’
6 means an engineered system that—

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

10 “(B) is designed to operate with varying
11 levels of adaptability and autonomy using ma-
12 chine and human-based inputs.”.

13 **SEC. 102. ONLINE CONTENT AUTHENTICITY AND PROVE-**
14 **NANCE STANDARDS RESEARCH AND DEVEL-**
15 **OPMENT.**

16 (a) RESEARCH.—

17 (1) IN GENERAL.—Not later than 180 days
18 after the date of the enactment of this Act, the
19 Under Secretary of Commerce for Standards and
20 Technology shall carry out research to facilitate the
21 development and standardization of means to pro-
22 vide authenticity and provenance information for
23 content generated by human authors and artificial
24 intelligence systems.

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

3 (A) Secure and binding methods for
4 human authors of content to append statements
5 of provenance through the use of unique cre-
6 dentials, watermarking, or other data or
7 metadata-based approaches.

8 (B) Methods for the verification of state-
9 ments of content provenance to ensure authen-
10 ticity such as watermarking or classifiers, which
11 are trained models that distinguish artificial in-
12 telligence-generated media.

13 (C) Methods for displaying clear and con-
14 spicuous statements of content provenance to
15 the end user.

16 (D) Technologies or applications needed to
17 facilitate the creation and verification of con-
18 tent provenance information.

19 (E) Mechanisms to ensure that any tech-
20 nologies and methods developed under this sec-
21 tion are minimally burdensome on content pro-
22 ducers.

23 (F) Such other related processes, tech-
24 nologies, or applications as the Under Secretary
25 considers appropriate.

1 (G) Use of provenance technology to en-
2 able attribution for content creators.

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

8 (b) DEVELOPMENT OF STANDARDS.—

9 (1) IN GENERAL.—For methodologies and ap-
10 plications related to content provenance and authen-
11 ticity deemed by the Under Secretary to be at a
12 readiness level sufficient for standardization, the
13 Under Secretary shall provide technical review and
14 assistance to such other Federal agencies and non-
15 governmental standards organizations as the Under
16 Secretary considers appropriate.

17 (2) CONSIDERATIONS.—In providing any tech-
18 nical review and assistance related to the develop-
19 ment of content provenance and authenticity stand-
20 ards under this subsection, the Under Secretary
21 may—

22 (A) consider whether a proposed standard
23 is reasonable, practicable, and appropriate for
24 the particular type of media and media environ-
25 ment for which the standard is proposed;

1 (B) consult with relevant stakeholders; and

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

4 (c) PILOT PROGRAM.—

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

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

16 (3) REQUIREMENTS.—In carrying out the pilot
17 program required by paragraph (1), the Under Sec-
18 retary shall—

19 (A) apply and evaluate methods for au-
20 thenticating the origin of and modifications to
21 government-produced digital content using tech-
22 nology and open standards described in para-
23 graph (1); and

24 (B) make available to the public digital
25 content embedded with provenance or other au-

1 thentication provided by the heads of the Fed-
2 eral agencies selected pursuant to paragraph
3 (2) for the purposes of the pilot program.

4 (4) BRIEFING REQUIRED.—Not later than 1
5 year after the date of the enactment of this Act, and
6 annually thereafter until the date described in para-
7 graph (5), the Under Secretary shall brief the Com-
8 mittee on Commerce, Science, and Transportation of
9 the Senate and the Committee on Science, Space,
10 and Technology of the House of Representatives on
11 the findings of the Under Secretary with respect to
12 the pilot program carried out under this subsection.

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

16 (d) REPORT TO CONGRESS.—Not later than 1 year
17 after the date of the enactment of this Act, the Under
18 Secretary shall submit to the Committee on Commerce,
19 Science, and Transportation of the Senate and the Com-
20 mittee on Science, Space, and Technology of the House
21 of Representatives a report outlining the progress of
22 standardization initiatives relating to requirements under
23 this section, as well as recommendations for legislative or
24 administrative action to encourage or require the wide-
25 spread adoption of such initiatives in the United States.

1 **SEC. 103. STANDARDS FOR DETECTION OF EMERGENT AND**
2 **ANOMALOUS BEHAVIOR AND AI-GENERATED**
3 **MEDIA.**

4 Section 22A(b)(1) of the National Institute of Stand-
5 ards and Technology Act (15 U.S.C. 278h–1(b)(1)) is
6 amended—

7 (1) by redesignating subparagraph (I) as sub-
8 paragraph (K);

9 (2) in subparagraph (H), by striking “; and”
10 and inserting a semicolon; and

11 (3) by inserting after subparagraph (H) the fol-
12 lowing:

13 “(I) best practices for detecting outputs
14 generated by artificial intelligence systems, in-
15 cluding content such as text, audio, images, and
16 videos;

17 “(J) methods to detect and understand
18 anomalous behavior of artificial intelligence sys-
19 tems and safeguards to mitigate potentially ad-
20 versarial or compromising anomalous behavior;
21 and”.

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

4 (a) IN GENERAL.—Not later than 1 year after the
5 date of enactment of this Act, the Comptroller General
6 of the United States shall—

7 (1) conduct a review of statutory, regulatory,
8 and other policy barriers to the use of artificial intel-
9 ligence systems to improve the functionality of the
10 Federal Government; and

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

14 (A) ensuring that an artificial intelligence
15 system is proportional to the need of the Fed-
16 eral Government;

17 (B) restrictions on access to and use of an
18 artificial intelligence system based on the capa-
19 bilities and risks of the artificial intelligence
20 system; and

21 (C) safety measures that ensure that an
22 artificial intelligence system is appropriately
23 limited to necessary data and compartmen-
24 talized from other assets of the Federal Govern-
25 ment.

1 (b) REPORT.—Not later than 2 years after the date
2 of enactment of this Act, the Comptroller General of the
3 United States shall submit to the Committee on Com-
4 merce, Science, and Transportation of the Senate and the
5 Committee on Science, Space, and Technology of the
6 House of Representatives a report that—

7 (1) summarizes the results of the review con-
8 ducted under subsection (a)(1) and the best prac-
9 tices identified under subsection (a)(2), including
10 recommendations, as the Comptroller General of the
11 United States considers appropriate;

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

17 (A) data analysis and processing;

18 (B) paperwork reduction;

19 (C) contracting and procurement practices;

20 and

21 (D) other Federal Government services;

22 and

23 (3) includes, as the Comptroller General of the
24 United States considers appropriate, recommenda-
25 tions to modify or eliminate barriers to the use of

1 artificial intelligence systems by the Federal Govern-
2 ment.

3 **TITLE II—ARTIFICIAL INTEL-**
4 **LIGENCE ACCOUNTABILITY**

5 **SEC. 201. DEFINITIONS.**

6 In this title:

7 (1) **APPROPRIATE CONGRESSIONAL COMMIT-**
8 **TEES.**—The term “appropriate congressional com-
9 mittees” means—

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

13 (B) the Committee on Energy and Com-
14 merce of the House of Representatives; and

15 (C) each congressional committee with ju-
16 risdiction over an applicable covered agency.

17 (2) **ARTIFICIAL INTELLIGENCE SYSTEM.**—The
18 term “artificial intelligence system” means an engi-
19 neered system that—

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

23 (B) is designed to operate with varying lev-
24 els of adaptability and autonomy using machine
25 and human-based inputs.

1 (3) COVERED AGENCY.—the term “covered
2 agency” means an agency for which the Under Sec-
3 retary develops an NIST recommendation.

4 (4) COVERED INTERNET PLATFORM.—

5 (A) IN GENERAL.—The term “covered
6 internet platform”—

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

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

14 (B) EXCLUSIONS.—The term “covered
15 internet platform” does not include a platform
16 that—

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

19 (I) during the most recent 180-
20 day period, did not employ more than
21 500 employees;

22 (II) during the most recent 3-
23 year period, averaged less than
24 \$50,000,000 in annual gross receipts;
25 and

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

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

7 (5) CRITICAL-IMPACT AI ORGANIZATION.—The
8 term “critical-impact AI organization” means a non-
9 government organization that serves as the deployer
10 of a critical-impact artificial intelligence system.

11 (6) CRITICAL-IMPACT ARTIFICIAL INTEL-
12 LIGENCE SYSTEM.—The term “critical-impact artifi-
13 cial intelligence system” means an artificial intel-
14 ligence system that—

15 (A) is deployed for a purpose other than
16 solely for use by the Department of Defense or
17 an intelligence agency (as defined in section
18 3094(e) of the National Security Act of 1947
19 (50 U.S.C. 3094(3))); and

20 (B) is used or intended to be used—

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

23 (I) the real-time or ex post facto
24 collection of biometric data of natural

1 persons by biometric identification
2 systems without their consent;

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

8 (III) criminal justice (as defined
9 in section 901 of title I of the Omni-
10 bus Crime Control and Safe Streets
11 Act of 1968 (34 U.S.C. 10251)); and

12 (ii) in a manner that poses a signifi-
13 cant risk to rights afforded under the Con-
14 stitution of the United States or safety.

15 (7) DEPLOYER.—The term “deployer”—

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

19 (B) does not include an entity that is sole-
20 ly an end user of a system.

21 (8) DEVELOPER.—The term “developer” means
22 an entity that—

23 (A) designs, codes, produces, or owns an
24 artificial intelligence system for internal use or

1 for use by a third party as a baseline model;
2 and

3 (B) does not act as a deployer of the artifi-
4 cial intelligence system described in subpara-
5 graph (A).

6 (9) GENERATIVE ARTIFICIAL INTELLIGENCE
7 SYSTEM.—The term “generative artificial intel-
8 ligence system” means an artificial intelligence sys-
9 tem that generates novel data or content in a writ-
10 ten, audio, or visual format.

11 (10) HIGH-IMPACT ARTIFICIAL INTELLIGENCE
12 SYSTEM.—The term “high-impact artificial intel-
13 ligence system” means an artificial intelligence sys-
14 tem—

15 (A) deployed for a purpose other than sole-
16 ly for use by the Department of Defense or an
17 intelligence agency (as defined in section
18 3094(e) of the National Security Act of 1947
19 (50 U.S.C. 3094(3))); and

20 (B) that is specifically developed with the
21 intended purpose of making decisions that have
22 a legal or similarly significant effect on the ac-
23 cess of an individual to housing, employment,
24 credit, education, healthcare, or insurance in a
25 manner that poses a significant risk to rights

1 afforded under the Constitution of the United
2 States or safety.

3 (11) NIST RECOMMENDATION.—The term
4 “NIST recommendation” means a sector-specific
5 recommendation developed under section 22B(b)(1)
6 of the National Institute of Standards and Tech-
7 nology Act, as added by section 204 of this Act.

8 (12) SECRETARY.—The term “Secretary”
9 means the Secretary of Commerce.

10 (13) SIGNIFICANT RISK.—The term “significant
11 risk” means a combination of severe, high-intensity,
12 high-probability, and long-duration risk of harm to
13 individuals.

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

17 (A) open, transparent, testable, and
18 verifiable specifications that characterize real-
19 istic operational performance, such as precision
20 and accuracy for relevant tasks;

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

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

1 (D) requirements for system validation and
2 integration into production environments, auto-
3 mated testing, and compliance with existing
4 legal and regulatory specifications;

5 (E) methods and tools for—

6 (i) the monitoring of system behavior;

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

9 (iii) the detection of emergent prop-
10 erties and related impacts; and

11 (F) and processes for redress and re-
12 sponse.

13 (15) UNDER SECRETARY.—The term “Under
14 Secretary” means the Director of the National Insti-
15 tute of Standards and Technology.

16 **SEC. 202. GENERATIVE ARTIFICIAL INTELLIGENCE TRANS-**
17 **PARENCY.**

18 (a) PROHIBITION.—

19 (1) IN GENERAL.—Subject to paragraph (2), it
20 shall be unlawful for a person to operate a covered
21 internet platform that uses a generative artificial in-
22 telligence system.

23 (2) DISCLOSURE OF USE OF GENERATIVE ARTI-
24 FICIAL INTELLIGENCE SYSTEMS.—

1 (A) IN GENERAL.—A person may operate
2 a covered internet platform that uses a genera-
3 tive artificial intelligence system if the person
4 provides notice to each user of the covered
5 internet platform that the covered internet plat-
6 form uses a generative artificial intelligence sys-
7 tem to generate content the user sees.

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

11 (i) subject to clause (ii), shall provide
12 the notice in a clear and conspicuous man-
13 ner on the covered internet platform before
14 the user interacts with content produced
15 by a generative artificial intelligence sys-
16 tem; and

17 (ii) may provide an option for the user
18 to choose to see the notice described in
19 clause (i) only upon the first interaction of
20 the user with content produced by a gen-
21 erative artificial intelligence system.

22 (b) ENFORCEMENT ACTION.—Upon learning that a
23 covered internet platform does not comply with the re-
24 quirements under this section, the Secretary—

25 (1) shall immediately—

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

3 (B) order the covered internet platform to
4 take remedial action to address the noncompli-
5 ance of the generative artificial intelligence sys-
6 tem operated by the covered internet platform;
7 and

8 (2) may, as determined appropriate or nec-
9 essary by the Secretary, take enforcement action
10 under section 208 if the covered internet platform
11 does not take sufficient action to remedy the non-
12 compliance within 15 days of the notification under
13 paragraph (1)(A).

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

17 **SEC. 203. TRANSPARENCY REPORTS FOR HIGH-IMPACT AR-**
18 **TIFICIAL INTELLIGENCE SYSTEMS.**

19 (a) TRANSPARENCY REPORTING.—

20 (1) IN GENERAL.—Each deployer of a high-im-
21 pact artificial intelligence system shall—

22 (A) before deploying the high-impact artifi-
23 cial intelligence system, and annually there-
24 after, submit to the Secretary a report describ-

1 ing the design and safety plans for the artificial
2 intelligence system; and

3 (B) submit to the Secretary an updated re-
4 port on the high-impact artificial intelligence
5 system if the deployer makes a material change
6 to—

7 (i) the purpose for which the high-im-
8 pact artificial intelligence system is used;
9 or

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

13 (2) CONTENTS.—Each transparency report sub-
14 mitted under paragraph (1) shall include, with re-
15 spect to the high-impact artificial intelligence sys-
16 tem—

17 (A) the purpose;

18 (B) the intended use cases;

19 (C) deployment context;

20 (D) benefits;

21 (E) a description of data that the high-im-
22 pact artificial intelligence system, once de-
23 ployed, processes as inputs;

24 (F) if available—

- 1 (i) a list of data categories and for-
2 mats the deployer used to retrain or con-
3 tinue training the high-impact artificial in-
4 telligence system;
- 5 (ii) metrics for evaluating the high-im-
6 pact artificial intelligence system perform-
7 ance and known limitations; and
- 8 (iii) transparency measures, including
9 information identifying to individuals when
10 a high-impact artificial intelligence system
11 is in use;
- 12 (G) processes and testing performed before
13 each deployment to ensure the high-impact arti-
14 ficial intelligence system is safe, reliable, and
15 effective;
- 16 (H) if applicable, an identification of any
17 third-party artificial intelligence systems or
18 datasets the deployer relies on to train or oper-
19 ate the high-impact artificial intelligence sys-
20 tem; and
- 21 (I) post-deployment monitoring and user
22 safeguards, including a description of the over-
23 sight process in place to address issues as
24 issues arise.

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

5 (c) CONSIDERATIONS.—In carrying out subsections
6 (a) and (b), a deployer or developer of a high-impact artifi-
7 cial intelligence system shall consider the best practices
8 outlined in the most recent version of the risk manage-
9 ment framework developed pursuant to section 22A(c) of
10 the National Institute of Standards and Technology Act
11 (15 U.S.C. 278h–1(c)).

12 (d) NONCOMPLIANCE AND ENFORCEMENT ACTION.—
13 Upon learning that a deployer of a high-impact artificial
14 intelligence system is not in compliance with the require-
15 ments under this section with respect to a high-impact ar-
16 tificial intelligence system, the Secretary—

17 (1) shall immediately—

18 (A) notify the deployer of the finding; and

19 (B) order the deployer to immediately sub-
20 mit to the Secretary the report required under
21 subsection (a)(1); and

22 (2) if the deployer fails to submit the report by
23 the date that is 15 days after the date of the notifi-
24 cation under paragraph (1)(A), may take enforce-
25 ment action under section 208.

1 (e) AVOIDANCE OF DUPLICATION.—

2 (1) IN GENERAL.—Pursuant to the
3 deconfliction of duplicative requirements under para-
4 graph (2), the Secretary shall ensure that the re-
5 quirements under this section are not unnecessarily
6 burdensome or duplicative of requirements made or
7 oversight conducted by a covered agency regarding
8 the non-Federal use of high-impact artificial intel-
9 ligence systems.

10 (2) DECONFLICTION OF DUPLICATIVE REQUIRE-
11 MENTS.—Not later than 90 days after the date of
12 the enactment of this Act, and annually thereafter,
13 the Secretary, in coordination with the head of any
14 relevant covered agency, shall complete the
15 deconfliction of duplicative requirements relating to
16 the submission of a transparency report for a high-
17 impact artificial intelligence system under this sec-
18 tion.

19 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
20 tion shall be construed to require a deployer of a high-
21 impact artificial intelligence system to disclose any infor-
22 mation, including data or algorithms—

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

25 (2) that is confidential business information; or

1 (3) that is privileged.

2 **SEC. 204. RECOMMENDATIONS TO FEDERAL AGENCIES FOR**
3 **RISK MANAGEMENT OF HIGH-IMPACT ARTIFI-**
4 **CIAL INTELLIGENCE SYSTEMS.**

5 The National Institute of Standards and Technology
6 Act (15 U.S.C. 278h-1) is amended by inserting after sec-
7 tion 22A the following:

8 **“SEC. 22B. RECOMMENDATIONS TO FEDERAL AGENCIES**
9 **FOR SECTOR-SPECIFIC OVERSIGHT OF ARTI-**
10 **FICIAL INTELLIGENCE.**

11 “(a) DEFINITION OF HIGH-IMPACT ARTIFICIAL IN-
12 TELLIGENCE SYSTEM.—In this section, the term ‘high-im-
13 pact artificial intelligence system’ means an artificial intel-
14 ligence system—

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

20 “(2) that is specifically developed with the in-
21 tended purpose of making decisions that have a legal
22 or similarly significant effect on the access of an in-
23 dividual to housing, employment, credit, education,
24 health care, or insurance in a manner that poses a

1 significant risk to rights afforded under the Con-
2 stitution of the United States or to safety.

3 “(b) SECTOR-SPECIFIC RECOMMENDATIONS.—Not
4 later than 1 year after the date of the enactment of the
5 Artificial Intelligence Research, Innovation, and Account-
6 ability Act of 2023, the Director shall—

7 “(1) develop sector-specific recommendations
8 for individual Federal agencies to conduct oversight
9 of the non-Federal, and, as appropriate, Federal use
10 of high-impact artificial intelligence systems to im-
11 prove the safe and responsible use of such systems;
12 and

13 “(2) not less frequently than biennially, update
14 the sector-specific recommendations to account for
15 changes in technological capabilities or artificial in-
16 telligence use cases.

17 “(c) REQUIREMENTS.—In developing recommenda-
18 tions under subsection (b), the Director shall use the vol-
19 untary risk management framework required by section
20 22A(c) to identify and provide recommendations to a Fed-
21 eral agency—

22 “(1) to establish regulations, standards, guide-
23 lines, best practices, methodologies, procedures, or
24 processes to facilitate oversight of non-Federal use
25 of high-impact artificial intelligence systems; and

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

3 “(d) RECOMMENDATIONS.—In developing rec-
4 ommendations under subsection (b), the Director may in-
5 clude the following:

6 “(1) Key design choices made during high-im-
7 pact artificial intelligence model development, includ-
8 ing rationale and assumptions made.

9 “(2) Intended use and users, other possible use
10 cases, including any anticipated undesirable or po-
11 tentially harmful use cases, and what good faith ef-
12 forts model developers can take to mitigate the use
13 of the system in harmful ways.

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

17 “(4) Sector-specific differences in what con-
18 stitutes acceptable high-impact artificial intelligence
19 model functionality and trustworthiness, metrics
20 used to determine high-impact artificial intelligence
21 model performance, and any test results reflecting
22 application of these metrics to evaluate high-impact
23 artificial intelligence model performance across dif-
24 ferent sectors.

1 “(5) Recommendations to support iterative de-
2 velopment of subsequent recommendations under
3 subsection (b).

4 “(e) CONSULTATION.—In developing recommenda-
5 tions under subsection (b), the Director shall, as the Di-
6 rector considers applicable and practicable, consult with
7 relevant covered agencies and stakeholders representing
8 perspectives from civil society, academia, technologists, en-
9 gineers, and creators.”.

10 **SEC. 205. OFFICE OF MANAGEMENT AND BUDGET OVER-**
11 **SIGHT OF RECOMMENDATIONS TO AGENCIES.**

12 (a) RECOMMENDATIONS.—

13 (1) IN GENERAL.—Not later than 1 year after
14 the date of enactment of this Act, the Under Sec-
15 retary shall submit to the Director, the head of each
16 covered agency, and the appropriate congressional
17 committees each NIST recommendation.

18 (2) AGENCY RESPONSES TO RECOMMENDA-
19 TIONS.—Not later than 90 days after the date on
20 which the Under Secretary submits a NIST rec-
21 ommendation to the head of a covered agency under
22 paragraph (1), the head of the covered agency shall
23 transmit to the Director a formal written response
24 to the NIST recommendation that—

1 (A) indicates whether the head of the cov-
2 ered agency intends to—

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

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

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

9 (B) includes—

10 (i) with respect to a formal written re-
11 sponse described in clause (i) or (ii) of sub-
12 paragraph (A), a copy of a proposed time-
13 table for completing the procedures de-
14 scribed in that clause;

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

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

1 (b) PUBLIC AVAILABILITY.—The Director shall make
2 a copy of each NIST recommendation and each written
3 formal response of a covered agency required under sub-
4 section (a)(2) available to the public at reasonable cost.

5 (c) REPORTING REQUIREMENTS.—

6 (1) ANNUAL SECRETARIAL REGULATORY STA-
7 TUS REPORTS.—

8 (A) IN GENERAL.—On the first February
9 1 occurring after the date of enactment of this
10 Act, and annually thereafter until the date de-
11 scribed in subparagraph (B), the head of each
12 covered agency shall submit to the Director a
13 report containing the regulatory status of each
14 NIST recommendation.

15 (B) CONTINUED REPORTING.—The date
16 described in this subparagraph is the date on
17 which the head of a covered agency—

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

20 (ii) determines and states in a report
21 required under subparagraph (A) that no
22 regulatory action should be taken with re-
23 spect to a NIST recommendation.

24 (2) COMPLIANCE REPORT TO CONGRESS.—On
25 April 1 of each year, the Director shall—

1 (A) review the reports received under para-
2 graph (1)(A); and

3 (B) transmit comments on the reports to
4 the heads of covered agencies and the appro-
5 priate congressional committees.

6 (3) FAILURE TO REPORT.—If, on March 1 of
7 each year, the Director has not received a report re-
8 quired under paragraph (1)(A) from the head of a
9 covered agency, the Director shall notify the appro-
10 priate congressional committees of the failure.

11 (d) TECHNICAL ASSISTANCE IN CARRYING OUT REC-
12 OMMENDATIONS.—The Under Secretary shall provide as-
13 sistance to the heads of covered agencies relating to the
14 implementation of the NIST recommendations the heads
15 of covered agencies intend to carry out.

16 (e) REGULATION REVIEW AND IMPROVEMENT.—The
17 Administrator of the Office of Information and Regulatory
18 Affairs of the Office of Management and Budget, in con-
19 sultation with the Under Secretary, shall develop and peri-
20 odically revise performance indicators and measures for
21 sector-specific regulation of artificial intelligence.

22 **SEC. 206. RISK MANAGEMENT ASSESSMENT FOR CRITICAL-**
23 **IMPACT ARTIFICIAL INTELLIGENCE SYS-**
24 **TEMS.**

25 (a) REQUIREMENT.—

1 (1) IN GENERAL.—Each critical-impact AI or-
2 organization shall perform a risk management assess-
3 ment in accordance with this section.

4 (2) ASSESSMENT.—Each critical-impact AI or-
5 organization shall—

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

11 (B) not less frequently than biennially dur-
12 ing the period beginning on the date of enact-
13 ment of this Act and ending on the date on
14 which the applicable critical-impact artificial in-
15 telligence system is no longer being made pub-
16 licly available by the critical-impact AI organi-
17 zation, as applicable, conduct an updated risk
18 management assessment that—

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

22 (ii) provides, to the extent practicable,
23 aggregate results of any significant devi-
24 ation from expected performance detailed
25 in the assessment performed under sub-

1 paragraph (A) or the most recent assess-
2 ment performed under this subparagraph.

3 (3) REVIEW.—

4 (A) IN GENERAL.—Not later than 90 days
5 after the date of completion of a risk manage-
6 ment assessment by a critical-impact AI organi-
7 zation under this section, the critical-impact AI
8 organization shall submit to the Secretary a re-
9 port—

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

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

14 (B) ADDITIONAL INFORMATION.—Subject
15 to subsection (d), the Secretary may request
16 that a critical-impact AI organization submit to
17 the Secretary any related additional or clari-
18 fying information with respect to a risk man-
19 agement assessment performed under this sec-
20 tion.

21 (4) LIMITATION.—The Secretary may not pro-
22 hibit a critical-impact AI organization from making
23 a critical-impact artificial intelligence system avail-
24 able to the public based on the review by the Sec-
25 retary of a report submitted under paragraph (3)(A)

1 or additional or clarifying information submitted
2 under paragraph (3)(B).

3 (b) ASSESSMENT SUBJECT AREAS.—Each assess-
4 ment performed by a critical-impact AI organization under
5 subsection (a) shall describe the means by which the crit-
6 ical-impact AI organization is addressing, through a docu-
7 mented TEVV process, the following categories:

8 (1) Policies, processes, procedures, and prac-
9 tices across the organization relating to transparent
10 and effective mapping, measuring, and managing of
11 artificial intelligence risks, including—

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

15 (B) how the organization integrates char-
16 acteristics of trustworthy artificial intelligence,
17 which include valid, reliable, safe, secure, resil-
18 ient, accountable, transparent, globally and lo-
19 cally explainable, interpretable, privacy-en-
20 hanced, and fair with harmful bias managed,
21 into organizational policies, processes, proce-
22 dures, and practices;

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

1 (D) how the organization establishes risk
2 management processes and outcomes through
3 transparent policies, procedures, and other con-
4 trols based on organizational risk priorities.

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

8 (A) how the context was established and
9 understood;

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

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

14 (3) A description of how the organization em-
15 ploys quantitative, qualitative, or mixed-method
16 tools, techniques, and methodologies to analyze, as-
17 sess, benchmark, and monitor artificial intelligence
18 risk, including—

19 (A) identification of appropriate methods
20 and metrics;

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

23 (C) mechanisms for tracking artificial in-
24 telligence system risks over time; and

1 (D) processes for gathering and assessing
2 feedback relating to the efficacy of measure-
3 ment.

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

7 (A) how artificial intelligence risks based
8 on assessments and other analytical outputs de-
9 scribed in paragraphs (2) and (3) are
10 prioritized, responded to, and managed;

11 (B) how strategies to maximize artificial
12 intelligence benefits and minimize negative im-
13 pacts were planned, prepared, implemented,
14 documented, and informed by input from rel-
15 evant artificial intelligence deployers;

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

18 (D) regular monitoring of risk treatments,
19 including response and recovery, and commu-
20 nication plans for the identified and measured
21 artificial intelligence risks, as applicable.

22 (c) DEVELOPER OBLIGATIONS.—The developer of a
23 critical-impact artificial intelligence system that agrees
24 through a contract or license to provide technology or serv-
25 ices to a deployer of the critical-impact artificial intel-

1 lligence system shall provide to the deployer of the critical-
2 impact artificial intelligence system the information rea-
3 sonably necessary for the deployer to comply with the re-
4 quirements under subsection (a), including—

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

8 (A) data size;

9 (B) data sources;

10 (C) copyrighted data; and

11 (D) personal identifiable information;

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

15 (A) input modality;

16 (B) output modality;

17 (C) model size; and

18 (D) model architecture;

19 (3) known capabilities, limitations, and risks of
20 the baseline artificial intelligence system of the de-
21 veloper at the time of the development of the artifi-
22 cial intelligence system; and

23 (4) documentation for downstream use, includ-
24 ing—

25 (A) a statement of intended purpose;

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

5 (C) a statement of the potential for devi-
6 ation from the intended purpose of the baseline
7 artificial intelligence system.

8 (d) TERMINATION OF OBLIGATION TO DISCLOSE IN-
9 FORMATION.—

10 (1) IN GENERAL.—The obligation of a critical-
11 impact AI organization to provide information, upon
12 request of the Secretary, relating to a specific as-
13 sessment category under subsection (b) shall end on
14 the date of issuance of a relevant standard applica-
15 ble to the same category of a critical-impact artifi-
16 cial intelligence system by—

17 (A) the Secretary under section 207(c)
18 with respect to a critical-impact artificial intel-
19 ligence system;

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

23 (C) a non-governmental standards organi-
24 zation, as determined appropriate by the Sec-
25 retary.

1 (2) EFFECT OF NEW STANDARD.—In adopting
2 any standard applicable to critical-impact artificial
3 intelligence systems under section 207(c), the Sec-
4 retary shall—

5 (A) identify the category under subsection

6 (b) to which the standard relates, if any; and

7 (B) specify the information that is no
8 longer required to be included in a report re-
9 quired under subsection (a) as a result of the
10 new standard.

11 (e) RULE OF CONSTRUCTION.—Nothing in this sec-
12 tion shall be construed to require a critical-impact AI or-
13 ganization, or permit the Secretary, to disclose any infor-
14 mation, including data or algorithms—

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

17 (2) that is confidential business information; or

18 (3) that is privileged.

19 **SEC. 207. CERTIFICATION OF CRITICAL-IMPACT ARTIFICIAL**
20 **INTELLIGENCE SYSTEMS.**

21 (a) ESTABLISHMENT OF ARTIFICIAL INTELLIGENCE
22 CERTIFICATION ADVISORY COMMITTEE.—

23 (1) IN GENERAL.—Not later than 180 days
24 after the date of enactment of this Act, the Sec-
25 retary shall establish an advisory committee to pro-

1 vide advice and recommendations on TEVV stand-
2 ards and the certification of critical-impact artificial
3 intelligence systems.

4 (2) DUTIES.—The advisory committee estab-
5 lished under this section shall advise the Secretary
6 on matters relating to the testing and certification
7 of critical-impact artificial intelligence systems, in-
8 cluding by—

9 (A) providing recommendations to the Sec-
10 retary on proposed TEVV standards to ensure
11 such standards—

12 (i) maximize alignment and interoper-
13 ability with standards issued by nongovern-
14 mental standards organizations and inter-
15 national standards bodies;

16 (ii) are performance-based and im-
17 pact-based; and

18 (iii) are applicable or necessary to fa-
19 cilitate the deployment of critical-impact
20 artificial intelligence systems in a trans-
21 parent, secure, and safe manner;

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

1 (C) upon completion of the review under
2 subparagraph (B), providing consensus rec-
3 ommendations to the Secretary on—

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

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

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

15 (3) COMPOSITION.—The advisory committee es-
16 tablished under this subsection shall be composed of
17 not more than 15 members with a balanced composi-
18 tion of representatives of the private sector, institu-
19 tions of higher education, and non-profit organiza-
20 tions, including—

21 (A) representatives of—

22 (i) institutions of higher education;

23 (ii) companies developing or operating
24 artificial intelligence systems;

- 1 (iii) consumers or consumer advocacy
2 groups; and
3 (iv) enabling technology companies;
4 and
5 (B) any other members the Secretary con-
6 siders to be appropriate.

7 (b) ARTIFICIAL INTELLIGENCE CERTIFICATION
8 PLAN.—

9 (1) IN GENERAL.—Not later than 1 year after
10 the date of enactment of this Act, the Secretary
11 shall establish a 3-year implementation plan for the
12 certification of critical-impact artificial intelligence
13 systems.

14 (2) PERIODIC UPDATE.—The Secretary shall
15 periodically update the plan established under para-
16 graph (1).

17 (3) CONTENTS.—The plan established under
18 paragraph (1) shall include—

19 (A) a methodology for gathering and using
20 relevant, objective, and available information re-
21 lating to TEVV;

22 (B) a process for considering whether pre-
23 scribing certain TEVV standards under sub-
24 section (c) for critical-impact artificial intel-

1 intelligence systems is appropriate, necessary, or du-
2 plicative of existing international standards;

3 (C) if TEVV standards are considered ap-
4 propriate, a process for prescribing such stand-
5 ards for critical-impact artificial intelligence
6 systems; and

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

10 (4) CONSULTATION.—In developing the plan re-
11 quired under paragraph (1), the Secretary shall con-
12 sult the following:

13 (A) The National Artificial Intelligence
14 Initiative Office.

15 (B) The interagency committee established
16 under section 5103 of the National Artificial
17 Intelligence Initiative Act of 2020 (15 U.S.C.
18 9413).

19 (C) The National Artificial Intelligence Ad-
20 visory Committee.

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

23 (E) Other departments, agencies, and in-
24 strumentalities of the Federal Government, as
25 considered appropriate by the Secretary.

1 (5) SUBMISSION TO CERTIFICATION ADVISORY
2 COMMITTEE.—Upon completing the initial plan re-
3 quired under this subsection and upon completing
4 periodic updates to the plan under paragraph (2),
5 the Secretary shall submit the plan to the advisory
6 committee established under subsection (a) for re-
7 view.

8 (6) SUBMISSION TO COMMITTEES OF CON-
9 GRESS.—Upon completing the plan required under
10 this subsection, the Secretary shall submit to the rel-
11 evant committees of Congress a report containing
12 the plan.

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

17 (c) STANDARDS.—

18 (1) STANDARDS.—

19 (A) IN GENERAL.—The Secretary shall
20 issue TEVV standards for critical-impact artifi-
21 cial intelligence systems.

22 (B) REQUIREMENTS.—Each standard
23 issued under this subsection shall—

24 (i) be practicable;

1 (ii) meet the need for safe, secure,
2 and transparent operations of critical-im-
3 pact artificial intelligence systems;

4 (iii) with respect to a relevant stand-
5 ard issued by a non-governmental stand-
6 ards organization that is already in place,
7 align with and be interoperable with that
8 standard;

9 (iv) provide for a mechanism to, not
10 less frequently than once every 2 years, so-
11 licit public comment and update the stand-
12 ard to reflect advancements in technology
13 and system architecture; and

14 (v) be stated in objective terms.

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

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

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

23 (ii) risk management assessments con-
24 ducted under section 206(a); and

1 (iii) any additional information pro-
2 vided to the Secretary pursuant to section
3 203(a)(1)(B);

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

9 (C) consult with relevant artificial intel-
10 ligence stakeholders and review industry stand-
11 ards issued by nongovernmental standards or-
12 ganizations;

13 (D) pursuant to paragraph (1)(B)(iii), con-
14 sider whether adoption of a relevant standard
15 issued by a nongovernmental standards organi-
16 zation as a TEVV standard is the most appro-
17 priate action; and

18 (E) consider whether the standard takes
19 into account—

20 (i) transparent, replicable, and objec-
21 tive assessments of critical-impact artificial
22 intelligence system risk, structure, capabili-
23 ties, and design;

1 (ii) the risk posed to the public by an
2 applicable critical-impact artificial intel-
3 ligence system; and

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

8 (3) CONSULTATION.—Before finalizing a TEVV
9 standard issued under this subsection, the Secretary
10 shall submit the TEVV standard to the advisory
11 committee established under subsection (a) for re-
12 view.

13 (4) PUBLIC COMMENT.—Before issuing any
14 TEVV standard under this subsection, the Secretary
15 shall provide an opportunity for public comment.

16 (5) COOPERATION.—In developing a TEVV
17 standard under this subsection, the Secretary may,
18 as determined appropriate, advise, assist, and co-
19 operate with departments, agencies, and instrumen-
20 talities of the Federal Government, States, and other
21 public and private agencies.

22 (6) EFFECTIVE DATE OF STANDARDS.—

23 (A) IN GENERAL.—The Secretary shall
24 specify the effective date of a TEVV standard

1 issued under this subsection in the order
2 issuing the standard.

3 (B) LIMITATION.—Subject to subpara-
4 graph (C), a TEVV standard issued under this
5 subsection may not become effective—

6 (i) during the 180-day period fol-
7 lowing the date on which the TEVV stand-
8 ard is issued; and

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

11 (C) EXCEPTION.—Subparagraph (B) shall
12 not apply to the effective date of a TEVV
13 standard issued under this section if the Sec-
14 retary—

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

18 (ii) publishes the reasons for the find-
19 ing under clause (i).

20 (7) RULE OF CONSTRUCTION.—Nothing in this
21 subsection shall be construed to authorize the Sec-
22 retary to impose any requirements on or take any
23 enforcement actions under this section or section
24 208 relating to a critical-impact AI organization be-

1 fore a TEVV standard relating to those require-
2 ments is prescribed.

3 (d) EXEMPTIONS.—

4 (1) AUTHORITY TO EXEMPT AND PROCE-
5 DURES.—

6 (A) IN GENERAL.—The Secretary may ex-
7 empt, on a temporary basis, a critical-impact
8 artificial intelligence system from a TEVV
9 standard issued under subsection (c) on terms
10 the Secretary considers appropriate.

11 (B) RENEWAL.—An exemption under sub-
12 paragraph (A)—

13 (i) may be renewed only on reapplica-
14 tion; and

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

17 (C) PROCEEDINGS.—

18 (i) IN GENERAL.—The Secretary may
19 begin a proceeding to grant an exemption
20 to a critical-impact artificial intelligence
21 system under this paragraph if the critical-
22 impact AI organization that deployed the
23 critical-impact artificial intelligence sys-
24 tems applies for an exemption or a renewal
25 of an exemption.

1 (ii) NOTICE AND COMMENT.—The
2 Secretary shall publish notice of the appli-
3 cation under clause (i) and provide an op-
4 portunity to comment.

5 (iii) FILING.—An application for an
6 exemption or for a renewal of an exemp-
7 tion under this paragraph shall be filed at
8 such time and in such manner and contain
9 such information as the Secretary may re-
10 quire.

11 (D) ACTIONS.—The Secretary may grant
12 an exemption under this paragraph upon find-
13 ing that—

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

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

22 (2) DISCLOSURE.—Not later than 30 days after
23 the date on which an application is filed under this
24 subsection, the Secretary may make public informa-
25 tion contained in the application or relevant to the

1 application, unless the information concerns or is re-
2 lated to a trade secret or other confidential informa-
3 tion not relevant to the application.

4 (3) NOTICE OF DECISION.—The Secretary shall
5 publish in the Federal Register a notice of each deci-
6 sion granting or denying an exemption under this
7 subsection and the reasons for granting or denying
8 that exemption, including a justification with sup-
9 porting information for the selected approach.

10 (e) SELF-CERTIFICATION OF COMPLIANCE.—

11 (1) IN GENERAL.—Subject to paragraph (2),
12 with respect to each critical-impact artificial intel-
13 ligence system of a critical-impact AI organization,
14 the critical-impact AI organization shall certify to
15 the Secretary that the critical-impact artificial intel-
16 ligence system complies with applicable TEVV
17 standards issued under this section.

18 (2) EXCEPTION.—A critical-impact AI organi-
19 zation may not issue a certificate under paragraph
20 (1) if, in exercising reasonable care, the critical-im-
21 pact AI organization has constructive knowledge
22 that the certificate is false or misleading in a mate-
23 rial respect.

24 (f) NONCOMPLIANCE FINDINGS AND ENFORCEMENT
25 ACTION.—

1 (1) FINDING OF NONCOMPLIANCE BY SEC-
2 RETARY.—Upon learning that a critical-impact arti-
3 ficial intelligence system deployed by a critical-im-
4 pact AI organization does not comply with the re-
5 quirements under this section, the Secretary shall—

6 (A) immediately—

7 (i) notify the critical-impact AI orga-
8 nization of the finding; and

9 (ii) order the critical-impact AI orga-
10 nization to take remedial action to address
11 the noncompliance of the artificial intel-
12 ligence system; and

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

20 (2) ACTIONS BY CRITICAL-IMPACT AI ORGANIZA-
21 TION.—If a critical-impact AI organization finds
22 that a critical-impact artificial intelligence system
23 deployed by the critical-impact AI organization is
24 noncompliant with an applicable TEVV standard
25 issued under this section or the critical-impact AI

1 organization is notified of noncompliance by the Sec-
2 retary under paragraph (1)(A)(i), the critical-impact
3 AI organization shall—

4 (A) without undue delay, notify the Sec-
5 retary by certified mail or electronic mail of the
6 noncompliance or receipt of the notification of
7 noncompliance;

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

10 (C) not later than 10 days after the date
11 of the notification or receipt under subpara-
12 graph (A), submit to the Secretary a report
13 containing information on—

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

17 (ii) measures taken to remedy such
18 noncompliance; and

19 (iii) actions taken by the critical-im-
20 pact AI organization to address stake-
21 holders affected by such noncompliance.

22 **SEC. 208. ENFORCEMENT.**

23 (a) IN GENERAL.—Upon discovering noncompliance
24 with a provision of this Act by a deployer of a high-impact
25 artificial intelligence system or a critical-impact AI organi-

1 zation if the Secretary determines that actions taken by
2 the critical-impact AI organization are insufficient to rem-
3 edy the noncompliance, the Secretary shall take an action
4 described in this section.

5 (b) CIVIL PENALTIES.—

6 (1) IN GENERAL.—The Secretary may impose a
7 penalty described in paragraph (2) on deployer of a
8 high-impact artificial intelligence system or a crit-
9 ical-impact AI organization for each violation by
10 that entity of this Act or any regulation or order
11 issued under this Act.

12 (2) PENALTY DESCRIBED.—The penalty de-
13 scribed in this paragraph is the greater of—

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

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

18 (c) VIOLATION WITH INTENT.—

19 (1) IN GENERAL.—If the Secretary determines
20 that a deployer of a high-impact artificial intel-
21 ligence system or a critical-impact AI organization
22 intentionally violates this Act or any regulation or
23 order issued under this Act, the Secretary may pro-
24 hibit the critical-impact AI organization from de-

1 plying a critical-impact artificial intelligence sys-
2 tem.

3 (2) IN ADDITION.—A prohibition imposed under
4 paragraph (1) shall be in addition to any other civil
5 penalties provided under this Act.

6 (d) FACTORS.—The Secretary may by regulation pro-
7 vide standards for establishing levels of civil penalty under
8 this section based upon factors such as the seriousness of
9 the violation, the culpability of the violator, and such miti-
10 gating factors as the violator’s record of cooperation with
11 the Secretary in disclosing the violation.

12 (e) CIVIL ACTION.—

13 (1) IN GENERAL.—Upon referral by the Sec-
14 retary, the Attorney General may bring a civil action
15 in a United States district court to—

16 (A) enjoin a violation of section 207; or

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

19 (2) VENUE.—A civil action may be brought
20 under paragraph (1) in the judicial district in which
21 the violation occurred or the defendant is found, re-
22 sides, or does business.

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

1 (f) RULE OF CONSTRUCTION.—Nothing in this sec-
2 tion shall be construed to require a developer of a critical-
3 impact artificial intelligence system to disclose any infor-
4 mation, including data or algorithms—

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

7 (2) that is confidential business information; or

8 (3) that is privileged.

9 **SEC. 209. ARTIFICIAL INTELLIGENCE CONSUMER EDU-**
10 **CATION.**

11 (a) ESTABLISHMENT.—Not later than 180 days after
12 the date of enactment of this Act, the Secretary shall es-
13 tablish a working group relating to responsible education
14 efforts for artificial intelligence systems.

15 (b) MEMBERSHIP.—

16 (1) IN GENERAL.—The Secretary shall appoint
17 to serve as members of the working group estab-
18 lished under this section not more than 15 individ-
19 uals with expertise relating to artificial intelligence
20 systems, including—

21 (A) representatives of—

22 (i) institutions of higher education;

23 (ii) companies developing or operating
24 artificial intelligence systems;

1 (iii) consumers or consumer advocacy
2 groups;

3 (iv) public health organizations;

4 (v) marketing professionals;

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

8 (vii) public safety organizations;

9 (viii) rural workforce development ad-
10 vocates;

11 (ix) enabling technology companies;

12 and

13 (x) nonprofit technology industry
14 trade associations; and

15 (B) any other members the Secretary con-
16 siders to be appropriate.

17 (2) COMPENSATION.—A member of the working
18 group established under this section shall serve with-
19 out compensation.

20 (c) DUTIES.—

21 (1) IN GENERAL.—The working group estab-
22 lished under this section shall—

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

1 (i) consumers and other stakeholders
2 with respect to artificial intelligence sys-
3 tems as those systems—

4 (I) become available; or

5 (II) are soon to be made widely
6 available for public use or consump-
7 tion; and

8 (B) submit to Congress, and make avail-
9 able to the public, a report containing the find-
10 ings and recommendations under subparagraph
11 (A).

12 (2) FACTORS FOR CONSIDERATION.—The work-
13 ing group established under this section shall take
14 into consideration topics relating to—

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

17 (B) use cases of artificial intelligence appli-
18 cations that improve lives of the people of the
19 United States, such as improving government
20 efficiency, filling critical roles, and reducing
21 mundane work tasks;

22 (C) artificial intelligence research break-
23 throughs;

24 (D) engagement and interaction methods,
25 including how to adequately inform consumers

1 of interaction with an artificial intelligence sys-
2 tem;

3 (E) human-machine interfaces;

4 (F) emergency fallback scenarios;

5 (G) operational boundary responsibilities;

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

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

10 (3) CONSULTATION.—The Secretary shall con-
11 sult with the Chair of the Federal Trade Commis-
12 sion with respect to the recommendations of the
13 working group established under this section, as ap-
14 propriate.

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

○