118TH CONGRESS
2D SESSION

# S. ____

To establish the Artificial Intelligence Safety Review Office in the Department of Commerce, and for other purposes.

---

## IN THE SENATE OF THE UNITED STATES

---

Mr. ROMNEY (for himself, Mr. REED, Mr. MORAN, Mr. KING, and Ms. HASSAN) introduced the following bill; which was read twice and referred to the Committee on _____

---

# A BILL

To establish the Artificial Intelligence Safety Review Office in the Department of Commerce, 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; TABLE OF CONTENTS.**

4     (a) SHORT TITLE.—This Act may be cited as the

5 "Preserving American Dominance in Artificial Intelligence

6 Act of 2024".

7     (b) TABLE OF CONTENTS.—The table of contents for

8 this Act is as follows:

2

**SEC. 2. FINDINGS; SENSE OF CONGRESS.**

(a) FINDINGS.—Congress finds the following:

(1) Advancements in artificial intelligence have the potential to dramatically improve and transform our way of life, but also present a broad spectrum of risks that could be harmful to the people of the United States.

(2) According to the United States Government, academia, and distinguished experts, advancements in artificial intelligence have the potential to be misused by bad actors.

(3) The Department of Defense, the Department of State, the intelligence community, and the National Security Commission on Artificial Intelligence, as well as senior officials at the Department of Energy, Argonne National Laboratory, the Cybersecurity and Infrastructure Security Agency, and the National Counterterrorism Center, have underscored that advanced artificial intelligence poses risks to United States national security, including through

1   enabling the development of biological, chemical,

2   cyber, radiological, or nuclear weapons.

3        (4) Advanced artificial intelligence models could

4   one day be leveraged by terrorists or adversarial na-

5   tion state regimes to cause widespread harm or

6   threaten United States national security.

7        (5) A September 2023 hearing titled, "Ad-

8   vanced Technology: Examining Threats to National

9   Security", held by the Subcommittee on Emerging

10  Threats and Spending Oversight of the Committee

11  on Homeland Security and Governmental Affairs of

12  the Senate, heard testimony that advanced artificial

13  intelligence models could facilitate or assist in the

14  development of extreme national security risks and

15  that the United States Government may lack au-

16  thorities to adequately respond to such risks posed

17  by broadly capable, general purpose frontier artifi-

18  cial intelligence models.

19  (b) SENSE OF CONGRESS.—It is the sense of Con-

20  gress that—

21       (1) the Federal Government should address ex-

22  treme risks posed by advanced artificial intelligence,

23  yet also ensure that the domestic artificial intel-

24  ligence industry is able to develop and maintain an

25  advantage over foreign adversaries; and

1        (2) the Federal Government should ensure that

2    any new requirements placed on industry do not bar

3    new entrants who will help drive innovation and dis-

4    covery.

**SEC. 3. DEFINITIONS.**

In this Act:

        (1) ALIEN.—The term "alien" has the meaning

    given such term in section 101 of the Immigration

    and Nationality Act (8 U.S.C. 1101).

        (2) COVERED DATA CENTER.—The term "cov-

    ered data center" means a set of physically co-lo-

    cated machines having a theoretical maximum com-

    puting capacity of 100,000,000,000,000,000,000 in-

    teger or floating-point operations per second, includ-

    ing those connected by data center networking at a

    rate of over 100 gigabits per second for training cov-

    ered frontier artificial intelligence models.

        (3) COVERED FRONTIER ARTIFICIAL INTEL-

    LIGENCE MODEL.—

            (A) IN GENERAL.—Except as provided in

        subparagraph (B), the term "covered frontier

        artificial intelligence model" means a type of

        artificial intelligence model that—

                (i) is trained with a total quantity of

            compute      power      greater      than

1          100,000,000,000,000,000,000,000,000 op-

2     erations;

3              (ii) is—

4                   (I) broadly capable, general-pur-

5              pose, and able to complete a variety of

6              downstream tasks; or

7                   (II) designed to produce outputs

8              relating to biology, chemistry, radio-

9              active materials, nuclear development,

10             or cyber capabilities; and

11             (iii) is accessible to users in the

12      United States.

13          (B) ALTERNATE DEFINITION.—Not less

14     frequently than every 2 years, the Secretary of

15     Commerce shall submit to Congress rec-

16     ommended changes, if any, to the definition of

17     the term "covered frontier artificial intelligence

18     model" under subparagraph (A) that shall be

19     based on capabilities of artificial intelligence

20     models to pose chemical, biological, radiological,

21     nuclear, or cyber risks as technological advance-

22     ments occur.

23     (4) COVERED FRONTIER ARTIFICIAL INTEL-

24     LIGENCE MODEL DEVELOPER.—The term "covered

25     frontier artificial intelligence model developer"

means a person who develops, trains, pre-trains or fine-tunes, or creates a covered frontier artificial intelligence model, including by taking steps to initiate a training run of the covered frontier artificial intelligence model.

(5) COVERED INTEGRATED CIRCUITS.—The term "covered integrated circuits" means—

(A) integrated circuits classified under Export Control Classification Number 3A090 or 3A001; or

(B) computers and other products classified under Export Control Classification Number 4A090 or 4A003.

(6) DEPLOY.—The term "deploy" means an action taken by a covered frontier artificial intelligence model developer to release, sell, or otherwise provide access to a covered frontier artificial intelligence model outside the custody of the developer, including by releasing an open source covered frontier artificial intelligence model.

(7) EXECUTIVE AGENCY.—The term "Executive agency" has the meaning given such term in section 1015 of title 5, United States Code.

1          (8) FOREIGN PERSON.—The term "foreign per-
2     son" means a person that is not a United States
3     person.

4          (9) INFRASTRUCTURE-AS-A-SERVICE PRO-
5     VIDER.—The term "infrastructure-as-a-service pro-
6     vider" means a person who sells or makes otherwise
7     available to customers infrastructure-as-a-service
8     products or services that provide cloud-based proc-
9     essing, storage, networks, or other fundamental com-
10    puting resources, and with which the consumer is
11    able to deploy and run software that is not
12    predefined, including operating systems and applica-
13    tions.

14         (10) LAWFULLY ADMITTED FOR PERMANENT
15    RESIDENCE.—The term "lawfully admitted for per-
16    manent residence" has the meaning given such term
17    in section 101 of the Immigration and Nationality
18    Act (8 U.S.C. 1101).

19         (11) OFFICE.—The term "Office" means the
20    Artificial Intelligence Safety Review Office estab-
21    lished pursuant to section 4(a).

22         (12) PERSON.—The term "person" means an
23    individual or entity.

24         (13) UNDER SECRETARY.—The term "Under
25    Secretary" means the Under Secretary of Commerce

1   for Artificial Intelligence Safety appointed under

2   section 4(d)(1).

3        (14) UNITED STATES PERSON.—The term

4   "United States person" means—

5            (A) a United States citizen or an alien law-

6        fully admitted for permanent residence to the

7        United States;

8            (B) an entity organized under the laws of

9        the United States or of any jurisdiction within

10       the United States, including a foreign branch of

11       such an entity; or

12           (C) a person in the United States.

13       (15) RED-TEAMING.—The term "red-teaming"

14   means structured adversarial testing efforts of a cov-

15   ered frontier artificial intelligence model to identify

16   risks, flaws, and vulnerabilities of an artificial intel-

17   ligence system, such as harmful outputs from the

18   system, unforeseen or undesirable system behaviors,

19   limitations, or potential risks associated with the

20   misuse of the model, related to chemical, biological,

21   radiological, nuclear, or cyber risks.

22   **SEC. 4. ESTABLISHMENT OF ARTIFICIAL INTELLIGENCE**

23                **SAFETY REVIEW OFFICE.**

24   (a) ESTABLISHMENT.—

1      (1) IN GENERAL.—Not later than 180 days

2   after the date of the enactment of this Act, the Sec-

3   retary of Commerce shall establish an office for the

4   purposes set forth under subsection (b).

5      (2) DESIGNATION.—The office established pur-

6   suant to paragraph (1) shall be known as the "Arti-

7   ficial Intelligence Safety Review Office".

8   (b) PURPOSES.—The purposes of the Office are as

9 follows:

10      (1) To oversee risks posed by covered frontier

11   artificial intelligence models relating to chemical, bi-

12   ological, radiological, nuclear, and cybersecurity

13   threats.

14      (2) To lead interagency efforts to implement

15   the requirements of this Act.

16      (3) To evaluate covered frontier artificial intel-

17   ligence models for compliance with the requirements

18   of this Act.

19      (4) To study and to submit to Congress reports

20   on unforeseen challenges and risks posed by ad-

21   vanced artificial intelligence.

22   (c) INTERAGENCY COORDINATION.—The Office shall

23 carry out the purposes set forth in subsection (b) and

24 functions of the Office set forth under subsection (e) in

25 coordination with the heads of each of the following:

1          (1) The Department of Energy.

2          (2) The Department of Homeland Security.

3          (3) The Department of Health and Human

4     Services.

5          (4) The Bureau of Industry and Security.

6          (5) The National Institute for Standards and

7     Technology.

8          (6) The National Nuclear Security Administra-

9     tion.

10          (7) The Cybersecurity and Infrastructure Secu-

11     rity Agency.

12          (8) The National Security Agency.

13          (9) Such other Executive agencies as the Presi-

14     dent considers appropriate.

15     (d) ORGANIZATION.—

16          (1) UNDER SECRETARY OF COMMERCE FOR AR-

17     TIFICIAL INTELLIGENCE SAFETY.—The President

18     shall appoint, by and with the advice and consent of

19     the Senate, an Under Secretary of Commerce for

20     Artificial Intelligence Safety, who shall—

21               (A) have experience and expertise in na-

22          tional security; and

23               (B) oversee the Office established in this

24          section.

1          (2) DETAILEES.—Each head of an Executive

2    agency set forth under subsection (c) shall detail or

3    assign to the Office 1 or more employees of the Ex-

4    ecutive agency for a period of not less than 1 year.

5          (3) OFFICERS AND EMPLOYEES.—

6               (A) IN GENERAL.—Except as otherwise

7          provided in this subsection, officers and employ-

8          ees of the Office shall be selected and appointed

9          by the Under Secretary, and shall be vested

10         with such powers and duties as the Under Sec-

11         retary may determine.

12              (B) ADMINISTRATIVELY DETERMINED EM-

13         PLOYEES.—

14                   (i) APPOINTMENT; COMPENSATION;

15              REMOVAL.—Of the officers and employees

16              employed by the Office under subpara-

17              graph (A), not more than 50 may be ap-

18              pointed, compensated, or removed without

19              regard to title 5, United States Code.

20                   (ii) ADDITIONAL POSITIONS.—Posi-

21              tions authorized by clause (i) shall be in

22              addition to those otherwise authorized by

23              law, including positions authorized under

24              section 5108 of title 5, United States

25              Code.

1          (iii) RATES OF PAY FOR OFFICERS

2       AND EMPLOYEES.—The Under Secretary

3       may set and adjust rates of basic pay for

4       officers and employees appointed under

5       clause (i) without regard to the provisions

6       of chapter 51 or subchapter III of chapter

7       53 of title 5, United States Code, relating

8       to classification of positions and General

9       Schedule pay rates, respectively.

10          (C) TECHNICAL EXPERTISE.—The Under

11     Secretary shall ensure that the staff of the Of-

12     fice has technical expertise in each of the fol-

13     lowing fields:

14          (i) Artificial intelligence.

15          (ii) Biotechnology.

16          (iii) Cybersecurity.

17          (iv) Physics.

18          (v) Such other fields as the Under

19       Secretary determines relevant to the ad-

20       ministration of the responsibilities of the

21       Office.

22     (e) FUNCTIONS.—The Under Secretary shall be re-

23  sponsible for the functions of the Office, which are as fol-

24  lows:

1      (1) To establish the reporting procedures re-

2   quired by section 5(a).

3      (2) To issue guidance in accordance with sec-

4   tion 5(b).

5      (3) To design the evaluation required by section

6   5(c)(1).

7      (4) To conduct pre-deployment reviews under

8   section 5(d).

9      (5) To issue regulations under section 5(f).

10 (f) BIENNIAL STUDIES.—Not later than 3 years after

11 the date of the enactment of this Act, and not less fre-

12 quently than once every 2 years thereafter, the Under Sec-

13 retary shall—

14      (1) conduct a study on unforeseen challenges

15   and new risks posed by advanced artificial intel-

16   ligence; and

17      (2) submit to Congress a report on the findings

18   of the Under Secretary with respect to the study

19   conducted under paragraph (1).

20 (g) CONGRESSIONAL REPORTING.—

21      (1) ORGANIZATION CHART AND MISSION-STATE-

22   MENT.—Not later than 180 days after the date on

23   which the Office is established, the Under Secretary

24   shall submit to Congress an initial organization

25   chart and mission statement for the Office.

1     (2) REPORT ON ACTIVITIES AND CHAL-

2 LENGES.—Not later than 1 year after the date on

3 which the Office is established, the Under Secretary

4 shall submit to Congress a report on the activities

5 of the Office and the challenges faced by the Office.

6     (3) SUBMITTAL OF RUBRIC.—Not later than 1

7 year after the date of the enactment of this Act, the

8 Under Secretary shall submit to Congress the stand-

9 ardized rubrics established under section 5(c)(1)(E).

10     (4) ANNUAL REPORTS.—

11         (A) IN GENERAL.—Each year, the Under

12         Secretary shall submit an annual report to Con-

13         gress on the activities of the Office.

14         (B) ELEMENTS.—Each report submitted

15         under subparagraph (A) shall include statistics

16         relating to the number of reviews conducted by

17         the Under Secretary under section 5(d), includ-

18         ing the outcomes of such reviews, for the period

19         covered by the report.

20 **SEC. 5. OVERSIGHT OF COVERED FRONTIER ARTIFICIAL IN-**

21          **TELLIGENCE MODELS, COVERED INTE-**

22          **GRATED CIRCUITS, AND INFRASTRUCTURE-**

23          **AS-A-SERVICE.**

24     (a) REPORTING PROCEDURES.—Not later than 1

25 year after the date of the enactment of this Act, the Under

1 Secretary shall, in coordination with the Under Secretary

2 of Commerce for Industry and Security, the Director of

3 the National Institute of Standards and Technology, the

4 Secretary of Energy, and the heads of such other entities

5 specified under subsection (c) as the Under Secretary con-

6 siders necessary, establish the following:

7     (1) Procedures for covered frontier artificial in-

8     telligence model developers to report on implementa-

9     tion of red-teaming and mitigation techniques re-

10     quired under section 8(c)(1)(A).

11     (2) Procedures for covered frontier artificial in-

12     telligence model developers to report on cybersecu-

13     rity standards that must be implemented, as re-

14     quired under section 8(c)(1)(B). Such procedures

15     may also include ways for the Office to verify such

16     implementation.

17     (3) Procedures for covered frontier artificial in-

18     telligence model developers to report on the imple-

19     mentation of requirements under section 8.

20     (4) Procedures for covered data centers to re-

21     port facilities in accordance with section 8(a).

22     (5) Procedures for sellers of covered integrated

23     circuits and infrastructure-as-a-service providers to

24     report on the implementation and adherence to

25     standards as required by section 8(b)(2).

1          (6) Procedures for how the Office shall ensure

2     the protection of proprietary or sensitive information

3     provided by persons pursuant to reporting require-

4     ments established under this Act.

5     (b) REQUIRED STANDARDS.—

6          (1) KNOW-YOUR-CUSTOMER STANDARDS.—

7               (A) IN GENERAL.—Not later than 1 year

8          after the date of the enactment of this Act, the

9          Under Secretary shall issue required know-

10         your-customer standards for sellers of covered

11         integrated circuit and providers of infrastruc-

12         ture-as-a-service to implement when transacting

13         with foreign persons.

14              (B) ELEMENTS.—The standards issued

15         pursuant to subparagraph (A) shall include, at

16         a minimum, standards for the following:

17                   (i) Collecting the following informa-

18              tion:

19                        (I) The name of the customer.

20                        (II) The Internet Protocol ad-

21                   dress, if applicable.

22                        (III) The location from where the

23                   purchased product will be used.

24                        (IV) Information on beneficial

25                   ownership.

              (V) Such other information as the Under Secretary and the Under Secretary of Commerce for Industry and Security considers appropriate.

            (ii) Privacy protections for personally identifiable information and proprietary information provided by customers.

            (iii) Retention of information described in clause (i).

            (iv) Identifying and reporting on potential customers or transactions that could pose national security risks.

        (2) STANDARDS FOR RED-TEAMING PRACTICES AND OTHER APPROPRIATE TECHNIQUES.—

            (A) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Under Secretary shall, in coordination with the Director of the National Institute of Standards and Technology, the Director of the Cybersecurity and Infrastructure Security Agency, and the Secretary of Energy, issue required standards for red-teaming practices and other appropriate techniques for covered frontier artificial intelligence model developers.

1          (B) LIMITATION.—The red-teaming prac-

2     tices and other appropriate techniques required

3     by subparagraph (A) shall only address meth-

4     ods to mitigate chemical, biological, radiological,

5     nuclear, and cyber risks from covered frontier

6     artificial intelligence models during the develop-

7     ment and training of such models, including

8     during data curation and processing.

9   (c) EVALUATIONS.—

10     (1) DESIGN.—

11          (A) IN GENERAL.—Not later than 1 year

12     after the date of the enactment of this Act, the

13     Under Secretary shall, in coordination with the

14     heads of entities specified under section 4(c),

15     design an evaluation that shall be used by a

16     person seeking to deploy a covered frontier arti-

17     ficial intelligence model to evaluate the model

18     before deployment of the model in accordance

19     with section 8(d).

20          (B) COMPONENTS.—In designing the eval-

21     uation under subparagraph (A), the Under Sec-

22     retary shall ensure the evaluation—

23               (i) includes a mechanism for assessing

24          capabilities of covered frontier artificial in-

25          telligence models to produce outputs that

1 pose chemical, biological, radiological, nu-

2 clear, and cyber risks in a manner that is

3 increased compared to baseline risk; and

4 (ii) can be used to assess certain fea-

5 tures of a covered frontier artificial intel-

6 ligence model, including an assessment of

7 the types of data on which the model is

8 trained and model weights.

9 (C) BASELINE RISK.—For purposes of the

10 evaluations to be designed under subparagraph

11 (A), the Under Secretary shall establish a level

12 of baseline risk, which shall be a measure of the

13 ability of a person to create a chemical, biologi-

14 cal, radiological, nuclear, or cyber threat with-

15 out access to a covered frontier artificial intel-

16 ligence model.

17 (D) LIMITATIONS.—The Under Secretary

18 may not require the use of evaluations under

19 subparagraph (A) to test for risks other than

20 chemical, biological, radiological, nuclear, or

21 cyber risks.

22 (E) STANDARDIZED RUBRICS.—The Under

23 Secretary shall establish standardized rubrics

24 for reviewing results of evaluations of covered

25 frontier artificial intelligence models conducted

1    using the evaluation designed under subpara-

2    graph (A) to assess whether the covered fron-

3    tier artificial intelligence model has incor-

4    porated sufficient safeguards against producing

5    outputs that pose chemical, biological, radio-

6    logical, nuclear, and cyber risks.

7        (2) IMPLEMENTATION.—Pursuant to regula-

8    tions promulgated under subsection (f), each person

9    seeking to deploy a covered frontier artificial intel-

10   ligence model shall—

11           (A) conduct an evaluation of the covered

12       frontier artificial intelligence model using the

13       evaluation designed under paragraph (1); and

14           (B) transmit to the Under Secretary the

15       results of the evaluation conducted under sub-

16       paragraph (A).

17   (d) PRE-DEPLOYMENT REVIEW.—

18       (1) REVIEWS.—

19           (A) AUTHORIZED.—Pursuant to receipt of

20       a notice under section 8(d)(2) from a person

21       seeking to deploy a covered frontier artificial in-

22       telligence model, the Under Secretary may ini-

23       tiate a review of the covered frontier artificial

24       intelligence model under this subsection.

1          (B) REQUIRED.—Pursuant to receipt of a

2     request submitted under subsection (e)(3) for a

3     rereview of a covered frontier artificial intel-

4     ligence model, the Under Secretary shall initiate

5     another review of the covered frontier artificial

6     intelligence model under this subsection.

7     (2) REVIEW ELEMENTS.—In carrying out a re-

8     view under paragraph (1) of a covered frontier arti-

9     ficial intelligence model for a person seeking to de-

10    ploy a covered frontier artificial intelligence model,

11    the Under Secretary shall—

12         (A) using the standardized rubrics estab-

13    lished under paragraph (1)(E) of subsection (c),

14    assess the results of the evaluation conducted

15    by the person in accordance with paragraph (2)

16    of such subsection;

17         (B) determine whether the person has suf-

18    ficiently mitigated against producing outputs

19    from such covered frontier artificial intelligence

20    model that pose chemical, biological, radio-

21    logical, nuclear, and cyber risks based on the

22    assessment conducted under subparagraph (A);

23    and

24         (C) ensure the person is in compliance

25    with any regulations promulgated by the Under

1 Secretary under subsection (f) or any other re-
2 quirement of this Act.

3     (3) INTERAGENCY PROCESS.—The Under Sec-
4 retary shall coordinate with the heads of the Execu-
5 tive agencies specified under section 4(c), as the
6 Under Secretary determines appropriate, to complete
7 reviews under this subsection.

8     (4) MATERIALS.—Upon request by the Under
9 Secretary, a person seeking to deploy a covered fron-
10 tier artificial intelligence model shall provide to the
11 Under Secretary such additional materials as the
12 Under Secretary considers necessary to conduct a
13 review under this subsection.

14     (5) TIMELINE.—Any review conducted—

15         (A) pursuant to paragraph (1)(A) shall be
16     completed before the end of the 90-day period
17     beginning on the date of the acceptance of writ-
18     ten notice under section 8(d)(2) by the Under
19     Secretary; and

20         (B) pursuant to paragraph (1)(B) shall be
21     completed before the end of the 90-day period
22     beginning on the date of the receipt of the re-
23     quest submitted for rereview under subsection
24     (e)(3) by the Under Secretary.

1       (6) NOTICE OF RESULTS.—If the Under Sec-

2 retary initiates a review for a person under para-

3 graph (1), the Under Secretary shall notify the per-

4 son of the results of a review on or before the date

5 that is 5 days after the date on which all action

6 under this subsection has been completed with re-

7 spect to the review.

8 (e) ACTIONS BY THE UNDER SECRETARY.—

9       (1) IN GENERAL.—The Under Secretary may

10 prohibit deployment of a covered frontier artificial

11 intelligence model if the Under Secretary—

12             (A) determines, pursuant to a review under

13            subsection (d), that the covered frontier artifi-

14            cial intelligence model poses insufficiently miti-

15            gated chemical, biological, radiological, nuclear,

16            or cyber risks to national security; and

17             (B) on or before the date that is 5 days

18            after the date on which all action under sub-

19            section (d) has been completed with respect to

20            the review, notifies the person seeking to deploy

21            the covered frontier artificial intelligence model

22            of the determination described in subparagraph

23            (A) of this paragraph.

24       (2) EXPLANATION.—For all determinations

25 made by the Under Secretary to prohibit the deploy-

1  ment of a covered frontier artificial intelligence

2  model by a person under paragraph (1), the Under

3  Secretary shall provide to the person an explanation

4  for such determination and such additional technical

5  feedback as the Under Secretary considers appro-

6  priate.

7      (3) REQUEST FOR REREVIEW.—Upon a deter-

8  mination by the Under Secretary to prohibit the de-

9  ployment of a covered frontier artificial intelligence

10  model by a person under paragraph (1)—

11          (A) the person may submit to the Under

12      Secretary a request for a rereview under sub-

13      section (d)(1) and in so doing shall submit to

14      the Under Secretary such materials as the

15      Under Secretary considers appropriate to obtain

16      another review under such subsection; and

17          (B) the Under Secretary shall give priority

18      to rereviews under subsection (d)(1) carried out

19      pursuant to requests submitted under subpara-

20      graph (A) of this paragraph.

21      (4) APPEALS.—

22          (A) PROCESS FOR APPEAL.—The Under

23      Secretary shall establish a process under which

24      a person who is prohibited under paragraph (1)

25      from deploying a covered frontier artificial in-

1     telligence model may request the Secretary to

2     review the determination.

3            (B) REVIEW.—The Secretary shall review

4       each determination for which a request is made

5       under clause (i) within 90 days and confirm or

6       change the determination as the Secretary con-

7       siders appropriate.

8     (f) REGULATIONS.—Not later than 1 year after the

9  date of the enactment of this Act, the Under Secretary

10 shall issue regulations to implement this section.

11 **SEC. 6. STRATEGIES, BEST PRACTICES, AND TECHNICAL AS-**

12            **SISTANCE FOR COVERED FRONTIER ARTIFI-**

13            **CIAL INTELLIGENCE MODEL DEVELOPERS.**

14    (a) IN GENERAL.—The Director of the National In-

15 stitute of Standards and Technology may, acting through

16 the Artificial Intelligence Safety Institute, make available

17 to the Office and to covered frontier artificial intelligence

18 model developers—

19            (1) mitigation strategies and best practices that

20       covered frontier artificial intelligence model devel-

21       opers can leverage to mitigate chemical, biological,

22       radiological, nuclear, and cyber risks; and

23            (2) technical assistance.

24    (b) REPORT.—Not later than 1 year after the date

25 of the enactment of this Act, the Director shall submit

1 to Congress a report on the status of the strategies, best

2 practices, and technical assistance made available under

3 subsection (a).

**SEC. 7. CYBERSECURITY STANDARDS FOR COVERED FRON-**

**TIER ARTIFICIAL INTELLIGENCE MODEL DE-**

**VELOPERS.**

7     (a) IN GENERAL.—The Director of the Cybersecurity

8 and Infrastructure Security Agency, in coordination with

9 the Director of the National Security Agency, the Director

10 of the National Institute for Standards and Technology,

11 and the Under Secretary, shall develop or identify cyberse-

12 curity standards for covered frontier artificial intelligence

13 model developers to implement in order to safeguard arti-

14 ficial intelligence model weights and other sensitive infor-

15 mation.

16     (b) USE OF CERTAIN IDENTIFIED BEST PRAC-

17 TICES.—In carrying out subsection (a), the Director of the

18 Cybersecurity and Infrastructure Security Agency may le-

19 verage best practices identified in any Joint Cybersecurity

20 Information bulletin determined relevant by the Director.

**SEC. 8. OTHER REQUIREMENTS.**

22     (a) REPORTING REQUIREMENTS FOR COVERED DATA

23 CENTERS.—

24         (1) REQUIREMENT.—Any person who owns a

25     covered data center shall report to the Under Sec-

1    retary any facilities owned by that person that are

2    covered data centers.

3         (2) ELEMENTS.—Reporting of a facility under

4    paragraph (1) shall include the following:

5              (A) The location of the facility.

6              (B) The name of the owner of the facility.

7    (b) REQUIREMENTS FOR SELLERS OF COVERED IN-

8    TEGRATED CIRCUITS AND INFRASTRUCTURE-AS-A-SERV-

9    ICE PROVIDERS.—Sellers of covered integrated circuits

10   and infrastructure-as-a-service providers shall—

11             (1) implement and adhere to the standards

12        issued pursuant to section 5(b)(1); and

13             (2) report to the Under Secretary on such im-

14        plementation and adherence.

15   (c) REQUIREMENTS FOR COVERED FRONTIER ARTI-

16   FICIAL INTELLIGENCE MODEL DEVELOPERS.—

17             (1) IN GENERAL.—A covered frontier artificial

18        intelligence model developer shall implement—

19                  (A) the standards issued by the Under

20             Secretary under section 5(b)(2) to mitigate

21             chemical, biological, radiological, nuclear, and

22             cyber risks; and

23                  (B) cybersecurity standards developed or

24             identified pursuant to section 7.

1      (2) REPORTING.—A covered frontier artificial

2   intelligence model developer shall report to the

3   Under Secretary on the implementation of guidance

4   and standards required under paragraph (1).

5      (d) REQUIREMENTS FOR PERSONS SEEKING TO DE-

6   PLOY A COVERED FRONTIER ARTIFICIAL INTELLIGENCE

7   MODEL.—Any person seeking to deploy a covered frontier

8   artificial intelligence model shall—

9          (1) conduct an evaluation of the covered fron-

10     tier artificial intelligence model in accordance with

11     section 5(c)(2); and

12         (2) provide written notification to the Under

13     Secretary and submit the findings of the person with

14     respect to the evaluation conducted under paragraph

15     (1).

16     (e) REGULATIONS FOR TIMELINES.—The Secretary

17  may issue regulations to establish timelines for the re-

18  quirements under this section.

19  **SEC. 9. ENFORCEMENT AND PENALTIES.**

20     (a) IN GENERAL.—No person may deploy a covered

21  frontier artificial intelligence model that has been prohib-

22  ited from deployment by the Under Secretary under sec-

23  tion 5(e).

1     (b) ENFORCEMENT.—The Attorney General may

2  seek appropriate relief in the district courts of the United

3  States in order to enforce the requirements of this Act.

4     (c) CRIMINAL PENALTIES.—Any person determined

5  to have knowingly deployed a covered frontier artificial in-

6  telligence model in violation of subsection (a) shall be sub-

7  ject to imprisonment for a period of not more than 10

8  years.

9     (d) CIVIL PENALTIES.—The Under Secretary shall

10  issue a fine of not more than $1,000,000 per day to a

11  person who is subject to a provision of this Act or a regu-

12  lation promulgated under this Act and who fails to comply

13  with such provision or regulation.

14  **SEC. 10. AUTHORIZATION OF APPROPRIATIONS.**

15     There is authorized to be appropriated to the Office

16  $50,000,000 to carry out this Act.