

.....  
(Original Signature of Member)

119TH CONGRESS  
2D SESSION

**H. R.** \_\_\_\_\_

To amend the Homeland Security Act of 2002 to require certain entities to maintain a technical capability with respect to shutting down certain technology, and for other purposes.

\_\_\_\_\_  
IN THE HOUSE OF REPRESENTATIVES

Mr. LIEU introduced the following bill; which was referred to the Committee  
on \_\_\_\_\_

\_\_\_\_\_  
**A BILL**

To amend the Homeland Security Act of 2002 to require certain entities to maintain a technical capability with respect to shutting down certain technology, 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 “AI Kill Switch Act”.

1 **SEC. 2. SHUTDOWN-CAPABILITY STANDARD AND GRAD-**  
2 **UATED DEPLOYMENT-CORRECTIONS FRAME-**  
3 **WORK WITH RESPECT TO CERTAIN TECH-**  
4 **NOLOGY.**

5 (a) IN GENERAL.—Subtitle A of title XXII of the  
6 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)  
7 is amended by adding at the end the following new section:

8 **“SEC. 2220F. SHUTDOWN-CAPABILITY STANDARD AND**  
9 **GRADUATED DEPLOYMENT-CORRECTIONS**  
10 **FRAMEWORK WITH RESPECT TO CERTAIN**  
11 **TECHNOLOGY.**

12 “(a) RULEMAKING.—

13 “(1) IN GENERAL.—Except as provided in para-  
14 graph (3), not later than 90 days after the date of  
15 the enactment of this section and annually there-  
16 after, the Secretary, acting through the Director,  
17 shall update by rule the definitions for the terms  
18 ‘covered entity’ and ‘covered technology’ in this sec-  
19 tion.

20 “(2) FACTORS.—In making a determination  
21 under paragraph (1), the Secretary shall consider  
22 the following factors:

23 “(A) The extent to which the costs to com-  
24 ply with this section might unduly burden a  
25 small business concern.

1           “(B) The need to cover entities the activi-  
2           ties of which have the potential to advance arti-  
3           ficial intelligence capabilities in national secu-  
4           rity, including with respect to cybersecurity and  
5           chemical, biological, radiological, or nuclear ca-  
6           pabilities.

7           “(C) The capabilities of covered tech-  
8           nology, the deployment of such technology, and  
9           the manner in which the model weights of such  
10          technology are made available.

11          “(D) Such other factors as the Secretary  
12          determines relevant.

13          “(3) EXEMPTION.—An entity is not a covered  
14          entity if such entity operates or makes available to  
15          a third party a covered technology for personal, aca-  
16          demic, or non-commercial utilization only.

17          “(b) SHUTDOWN CAPABILITY.—

18                 “(1) IN GENERAL.—Not later than 90 days  
19                 after the date of the enactment of this section and  
20                 annually thereafter, the Secretary, acting through  
21                 the Director, shall by rule require a covered entity  
22                 to carry out the following:

23                         “(A) Maintain a technical capability to  
24                         carry out the following actions:

1 “(i) Stop inference of a covered tech-  
2 nology of such covered entity.

3 “(ii) Terminate user access to such  
4 technology.

5 “(iii) Suspend access to such tech-  
6 nology with respect to an account, user, or  
7 use pattern identified by such covered enti-  
8 ty or the Secretary as posing a risk of any  
9 of the following:

10 “(I) A covered incident.

11 “(II) A violation of law or the  
12 terms of service of such technology.

13 “(iv) Shut down such technology.

14 “(B) Not later than 15 days after such  
15 covered entity becomes aware of a covered inci-  
16 dent relating to such technology, submit to the  
17 Secretary a report regarding such incident.

18 “(2) CONSIDERATION.—In carrying out para-  
19 graph (1), the Secretary shall consider the following:

20 “(A) Requiring a technical capability based  
21 on a graduated deployment-corrections frame-  
22 work that applies when there is evidence of a  
23 credible risk of a covered incident and includes  
24 measures that are calibrated to the severity and

1 immediacy of such risk, including the following  
2 measures:

3 “(i) Throttling or otherwise altering  
4 any of the following:

5 “(I) The inference rate of a cov-  
6 ered technology.

7 “(II) User access to such tech-  
8 nology.

9 “(III) Compute allocation with  
10 respect to such technology.

11 “(ii) Disabling or restricting a capa-  
12 bility of such technology.

13 “(iii) Suspending such technology.

14 “(iv) Shutting down such technology.

15 “(v) Transitioning an operation de-  
16 pendent on such technology to a backup  
17 system or an earlier version of such tech-  
18 nology.

19 “(B) The risk that such a measure could  
20 disrupt critical infrastructure.

21 “(3) VOLUNTARY STANDARDS.—Not later than  
22 180 days after the date of the enactment of this sec-  
23 tion, the Secretary, acting through the Director,  
24 shall publish on a publicly available website of the

1 Agency voluntary standards for shutting down a cov-  
2 ered technology.

3 “(c) EMERGENCY AUTHORITY.—

4 “(1) ORDER.—If the Secretary, acting through  
5 the Director and in consultation with the Secretary  
6 of Commerce and the Director of National Intel-  
7 ligence, determines that a covered incident has oc-  
8 curred, the Secretary may order the covered entity  
9 at issue to take action proportionate to the nature  
10 and immediacy of such incident, which may include  
11 any of the actions described in subsection (b)(1)(A).

12 “(2) COVERED ENTITY.—Upon an order under  
13 paragraph (1), the covered entity subject to such  
14 order shall as soon as practicable carry out the fol-  
15 lowing:

16 “(A) Preserve the model weights and te-  
17 lemetry of such technology.

18 “(B) Notify to the extent practicable each  
19 operator or user of such technology, of the fol-  
20 lowing:

21 “(i) Such order.

22 “(ii) The extent to which such oper-  
23 ator or user, as the case may be, might be  
24 affected by such order.

1                   “(C) Confirm to the Secretary that such  
2                   order has been carried out.

3                   “(3) AUDIT.—Upon a confirmation under para-  
4                   graph (2)(C), the Secretary, acting through the Di-  
5                   rector, shall through audit, telemetry, on-site inspec-  
6                   tion, or other forensic review verify compliance with  
7                   the order that prompted such confirmation.

8                   “(4) CONGRESSIONAL REPORT.—Upon an order  
9                   under paragraph (1), the Secretary shall submit to  
10                  Congress a report regarding the covered incident at  
11                  issue that includes information relating to the fol-  
12                  lowing:

13                  “(A) The determination under such para-  
14                  graph that prompted such order.

15                  “(B) Each action so ordered.

16                  “(C) The covered entity subject to such  
17                  order.

18                  “(5) APPEAL.—

19                  “(A) IN GENERAL.—Not later than 48  
20                  hours after an order under paragraph (1), the  
21                  covered entity subject to such order may peti-  
22                  tion the Secretary for reconsideration of such  
23                  order, but such petition does not stay such  
24                  order.

1           “(B) DETERMINATION.—Not later than  
2           five days after a covered entity petitions pursu-  
3           ant to subparagraph (A), the Secretary, acting  
4           through the Director, shall make a determina-  
5           tion with respect to such petition, but if the  
6           Secretary fails to so make such determination,  
7           such failure is deemed to be a determination in  
8           the negative.

9           “(C) JUDICIAL REVIEW.—A covered entity  
10          for which there is an order under paragraph (1)  
11          may request review of such order in the United  
12          States Court of Appeals for the District of Co-  
13          lumbia Circuit on petition filed not later than  
14          60 days after such order.

15       “(d) AUTHORITY.—

16           “(1) IN GENERAL.—With respect to this sec-  
17          tion, the Secretary, acting through the Director,  
18          may carry out any of the following:

19           “(A) Administer oaths and, by subpoena,  
20          require testimony and the production of docu-  
21          ments.

22           “(B) Conduct an investigation within the  
23          United States and, consistent with applicable  
24          law, outside the United States.

25       “(2) CIVIL PENALTIES.—

1           “(A) IN GENERAL.—Except as provided in  
2           subparagraph (B), if the Secretary, acting  
3           through the Director, determines after reason-  
4           able notice and opportunity for a hearing that  
5           a covered entity has violated this section, the  
6           Secretary may assess on such covered entity a  
7           civil penalty of not more than \$2,000,000 for  
8           each day on which such violation occurs.

9           “(B) ORDER.—If the Secretary, acting  
10          through the Director, determines after reason-  
11          able notice and opportunity for a hearing that  
12          a covered entity has violated subsection (c), the  
13          Secretary may assess on such covered entity a  
14          civil penalty of not more than \$20,000,000 for  
15          each day on which such violation occurs.

16          “(C) FACTORS.—In determining the  
17          amount of a civil penalty to be assessed under  
18          subparagraph (A) or (B), the Secretary shall  
19          consider the following factors:

20                 “(i) The nature, circumstances, ex-  
21                 tent, gravity, and duration of the violation  
22                 at issue.

23                 “(ii) The degree of culpability of the  
24                 covered entity at issue.

1                   “(iii) Previous violations, if any, of  
2                   this section by such covered entity.

3                   “(iv) Good-faith efforts, if any, by  
4                   such covered entity to comply with this  
5                   section.

6                   “(v) Whether such covered entity vol-  
7                   untarily disclosed to the Secretary such  
8                   violation.

9                   “(vi) Any other factor that justice  
10                  may require.

11                 “(3) CIVIL ACTION.—If the Secretary, acting  
12                 through the Director, believes that a violation of this  
13                 section has occurred, is occurring, or is about to  
14                 occur, the Secretary may refer the matter to the At-  
15                 torney General to bring in an appropriate district  
16                 court of the United States a civil action for appro-  
17                 priate relief.

18                 “(e) COMPLIANCE.—A de minimis violation of this  
19                 section, or a technical defect that results in a violation  
20                 of this section, that is corrected not later than 30 days  
21                 after discovery of such violation or defect, as the case may  
22                 be, is not considered a violation of this section.

23                 “(f) NON-DISCLOSURE.—Nonpublic information sub-  
24                 mitted under this section to the Secretary by a covered  
25                 entity is exempt from disclosure under section 552(b)(3)

1 of title 5, United States Code, and from any provision of  
2 State, local, or Tribal freedom of information law, open  
3 government law, open records law, or similar law relating  
4 to the disclosure of information or records.

5 “(g) DEFINITIONS.—In this section:

6 “(1) AFFILIATE.—The term ‘affiliate’ means an  
7 entity that controls, is controlled by, or is under  
8 common control with, another entity.

9 “(2) ARTIFICIAL INTELLIGENCE.—The term  
10 ‘artificial intelligence’ has the meaning given such  
11 term in section 5002 of the National Artificial Intel-  
12 ligence Initiative Act of 2020 (15 U.S.C. 9401).

13 “(3) ARTIFICIAL INTELLIGENCE SYSTEM.—The  
14 term ‘artificial intelligence system’ means any of the  
15 following:

16 “(A) Artificial intelligence.

17 “(B) A system, software, hardware, tool,  
18 or other utility that operates autonomously  
19 through the utilization of such artificial intel-  
20 ligence.

21 “(4) COVERED ENTITY.—Except as otherwise  
22 provided in this section, the term ‘covered entity’  
23 means an entity that satisfies the following require-  
24 ments:

1           “(A) Operates a covered technology or op-  
2           erates a system that incorporates such tech-  
3           nology.

4           “(B) Makes such technology available to a  
5           third party through a programmatic interface,  
6           hosted service, or other similar mechanism.

7           “(C) Derives together with the affiliates, if  
8           any, of such person not less than \$500,000,000  
9           in gross revenue from such technology in the  
10          calendar year preceding the calendar year at  
11          issue.

12          “(5) COVERED INCIDENT.—The term ‘covered  
13          incident’ means an occurrence of any of the fol-  
14          lowing outside of red-teaming or other structured  
15          testing:

16               “(A) Sabotage of, or interference with, a  
17               lawful instruction to shut down a covered tech-  
18               nology.

19               “(B) Conduct of such technology that is  
20               unintended by a developer or operator of such  
21               technology and causes the death of not fewer  
22               than 10 individuals or economic damages of not  
23               less than \$100,000,000.

24               “(C) Concealment of a capability, inten-  
25               tion, or action of such technology, by such tech-

1 nology, from a monitoring or shutdown mecha-  
2 nism.

3 “(D) A loss-of-control scenario.

4 “(6) COVERED TECHNOLOGY.—Except as oth-  
5 erwise provided in this section, the term ‘covered  
6 technology’ means an artificial intelligence system  
7 developed utilizing a quantity of computing power  
8 the cost of which would exceed \$100,000,000 at the  
9 prevailing market price of cloud computing in the  
10 United States, as determined by the Secretary.

11 “(7) LOSS-OF-CONTROL SCENARIO.—The term  
12 ‘loss-of-control scenario’ means a scenario in which  
13 a covered technology pursues outside of red-teaming  
14 or other structured testing a goal that is not a goal  
15 intended by the developer or operator of such tech-  
16 nology, including with respect to any of the fol-  
17 lowing:

18 “(A) Such technology behaving contrary to  
19 the instruction of such developer or operator, as  
20 the case may be, in a context relating to critical  
21 infrastructure or another high-stakes context.

22 “(B) Such technology altering operational  
23 rules or safety restrictions without the author-  
24 ization of such developer or operator, as the  
25 case may be.

1           “(C) Such technology subverting a moni-  
2           toring or shutdown mechanism.

3           “(D) Such technology attaining without  
4           such authorization access to the model weights  
5           of such technology.

6           “(8) RED-TEAMING.—The term ‘red-teaming’  
7           means structured testing that satisfies the following  
8           requirements:

9           “(A) Is in a controlled environment.

10          “(B) Simulates real-world conditions.

11          “(C) Utilizes an adversarial method to  
12          identify limitations, risks, flaws and  
13          vulnerabilities with respect to an artificial intel-  
14          ligence system, such as any of the following:

15               “(i) A harmful output of such system.

16               “(ii) An unforeseen or undesirable be-  
17               havior of such system.

18               “(iii) A risk associated with the  
19               misutilization of such system.

20          “(9) SMALL BUSINESS CONCERN.—The term  
21          ‘small business concern’ has the meaning given such  
22          term in section 3 of the Small Business Act (15  
23          U.S.C. 632).”.

24          (b) CLERICAL AMENDMENT.—The table of contents  
25          in section 1(b) of the Homeland Security Act of 2002 is

- 1 amended by inserting after the item relating to section
- 2 2220E the following new item:

“Sec. 2220F. Shutdown-capability standard and graduated deployment-corrections framework with respect to certain technology.”.