

.....
(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To require the National Institute of Standards and Technology to carry out certain activities regarding certain artificial intelligence attacks, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. HARRIGAN introduced the following bill; which was referred to the Committee on _____

A BILL

To require the National Institute of Standards and Technology to carry out certain activities regarding certain artificial intelligence attacks, 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 Cyber Defense
5 Act”.

6 **SEC. 2. NIST AI DISTILLATION AND CYBERSECURITY**
7 **STANDARDS.**

8 (a) IN GENERAL.—

1 (1) ENGAGEMENT.—Not later than 180 days
2 after the date of the enactment of this Act, the Di-
3 rector of the National Institute of Standards and
4 Technology (NIST) shall seek to engage with private
5 sector artificial intelligence stakeholders to establish
6 the following:

7 (A) A definition for artificial intelligence
8 distillation attacks.

9 (B) Voluntary standards and best practices
10 for the detection and prevention of such at-
11 tacks.

12 (2) PUBLICATION.—Not later than one year
13 after the establishment of voluntary standards and
14 best practices under paragraph (1), the Director
15 shall publish on the website of NIST such voluntary
16 standards and best practices.

17 (b) STANDARDS AND BEST PRACTICES.—Not later
18 than 180 days after the date of the enactment of this Act,
19 the Director of NIST shall establish a roundtable, to be
20 known as the “AI Cybersecurity Roundtable” (in this sub-
21 section referred to as the “Roundtable”), to develop vol-
22 untary standards and best practices relating to the defen-
23 sive use of artificial intelligence for cybersecurity pur-
24 poses. The Director shall seek representation on the
25 Roundtable of private sector artificial intelligence stake-

1 holders and owners and operators of critical infrastruc-
2 ture. Not later than one year after the establishment of
3 the Roundtable, the Director shall publish on the website
4 of NIST such voluntary standards and best practices.

5 (c) DEFINITIONS.—In this section:

6 (1) ARTIFICIAL INTELLIGENCE.—The term “ar-
7 tificial intelligence” has the meaning given such
8 term in section 5002 of the Artificial Intelligence
9 Initiative Act of 2020 (15 U.S.C. 9401).

10 (2) COUNTRY OF CONCERN.—The term “coun-
11 try of concern” means—

12 (A) The People’s Republic of China, in-
13 cluding the Hong Kong and Macau Special Ad-
14 ministrative Regions.

15 (B) The Russian Federation;

16 (C) The Islamic Republic of Iran.

17 (D) The Democratic People’s Republic of
18 Korea.

19 (E) The Republic of Cuba.

20 (3) CRITICAL INFRASTRUCTURE.—The term
21 “critical infrastructure” has the meaning given such
22 term in section 1016(e) of Public Law 107–56 (42
23 U.S.C. 5195c(e)).

24 (4) ENTITY OF CONCERN.—

1 (A) IN GENERAL.—The term “entity of
2 concern” means any foreign person or entity
3 that—

4 (i) is headquartered in, or the parent
5 company of which is headquartered in, a
6 country of concern;

7 (ii) is operating under the direction or
8 control of any entity headquartered in, or
9 the parent company of which is
10 headquartered in, a country of concern; or

11 (iii) the Director of NIST determines
12 to be an entity of concern for purposes of
13 this section.

14 (B) EXCEPTION.—The term “entity of
15 concern” does not include a person who—

16 (i) lawfully admitted for permanent
17 residence (as such term is defined in sec-
18 tion 101(a) of the Immigration and Na-
19 tionality Act (8 U.S.C. 1101(a))); or

20 (ii) a citizen of the United States.

21 (5) PRIVATE SECTOR ARTIFICIAL INTEL-
22 LIGENCE STAKEHOLDERS.—The term “private sec-
23 tor artificial intelligence stakeholders” means any
24 corporation, partnership, limited liability company,
25 sole proprietorship, or other business entity that—

1 (A) is not a unit, agency, instrumentality,
2 or wholly-owned enterprise of a Federal, State,
3 local, or Tribal government;

4 (B) develops, trains, deploys, offers, sells,
5 or licenses one or more artificial intelligence
6 systems, or provides substantial computing in-
7 frastructure, data, or technical services for the
8 development or deployment of such systems, as
9 part of its ordinary business activities does so
10 for commercial purposes, including for profit, in
11 exchange for consideration, or in furtherance of
12 a business enterprise, regardless of whether
13 such entity has yet generated revenue; and

14 (C) is not an entity of concern.