....
(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. 9720

To direct the Director of the National Institute of Standards and Technology to update the national vulnerability database to reflect vulnerabilities to artificial intelligence systems, study the need for voluntary reporting related to artificial intelligence security and safety incidents, and for other purposes.

_____

IN THE HOUSE OF REPRESENTATIVES

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

_____

A BILL

To direct the Director of the National Institute of Standards and Technology to update the national vulnerability database to reflect vulnerabilities to artificial intelligence systems, study the need for voluntary reporting related to artificial intelligence security and safety incidents, 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,*

SECTION 1. SHORT TITLE.

This Act may be cited as the "AI Incident Reporting and Security Enhancement Act".

SEC. 2. ACTIVITIES TO SUPPORT VOLUNTARY VULNER- ABILITY AND INCIDENT TRACKING ASSOCI- ATED WITH ARTIFICIAL INTELLIGENCE.

(a) UPDATE TO NATIONAL VULNERABILITY DATA-BASE.—Subject to the availability of appropriations, the Director of the National Institute of Standards and Technology, in coordination with industry stakeholders, standards development organizations, and appropriate Federal agencies, as appropriate, shall carry out the following:

(1) Establish or identify common definitions and any characteristics of artificial intelligence security vulnerabilities that make utilization of the National Vulnerability Database inappropriate for the management of such vulnerabilities, and develop processes and procedures for vulnerability management of such vulnerabilities.

(2) Support the development of standards and guidance for technical vulnerability management processes related to artificial intelligence.

(3) Consistent with paragraphs (1) and (2), as appropriate, initiate a process to update the Institute's processes and procedures associated with the National Vulnerability Database to ensure such

1 Database and associated vulnerability management
2 processes incorporate artificial intelligence security
3 vulnerabilities to the greatest extent practicable.

4 (b) ASSESSING VOLUNTARY TRACKING OF SUBSTAN-
5 TIAL ARTIFICIAL INTELLIGENCE SECURITY AND SAFETY
6 INCIDENTS.—

7 (1) IN GENERAL.—Subject to the availability of
8 appropriations, the Director of the National Insti-
9 tute of Standards and Technology, in consultation
10 with the Director of the Cybersecurity and Infra-
11 structure Security Agency of the Department of
12 Homeland Security, shall convene a multi-stake-
13 holder process to consider the development of a
14 process relating to the voluntary collection, report-
15 ing, and tracking of substantial artificial intelligence
16 security incidents and substantial artificial intel-
17 ligence safety incidents.

18 (2) ACTIVITIES.—In carrying out paragraph
19 (1), the Director of the National Institute of Stand-
20 ards and Technology shall convene appropriate rep-
21 resentatives of industry, academia, nonprofit organi-
22 zations, standards development organizations, civil
23 society groups, Sector Risk Management Agencies,
24 and appropriate Federal departments and agencies
25 to carry out the following:

1   (A) Establish common definitions and
2 characterizations for relevant aspects of sub-
3 stantial artificial intelligence security incidents
4 and substantial artificial intelligence safety inci-
5 dents, which may include the following:

6   (i) Classifications that sufficiently dif-
7 ferentiate between the following:

8   (I) Artificial intelligence security
9 incidents.

10   (II) Artificial intelligence safety
11 incidents.

12   (ii) Taxonomies to classify incidents
13 referred to in clause (i) based on relevant
14 characteristics, impacts, or other appro-
15 priate criteria.

16   (B) Assess the usefulness and cost-effec-
17 tiveness of an effort to voluntarily track sub-
18 stantial artificial intelligence security incidents
19 and substantial artificial intelligence safety inci-
20 dents.

21   (C) Identify and provide guidelines, best
22 practices, methodologies, procedures, and proc-
23 esses for tracking and reporting substantial ar-
24 tificial intelligence security incidents and sub-

1 stantial artificial intelligence safety incidents

2 across different sectors and use cases.

3 (D) Support the development of standard-

4 ized reporting and documentation mechanisms,

5 including automated mechanisms, that would

6 help provide information, including public infor-

7 mation, regarding substantial artificial intel-

8 ligence security incidents and substantial artifi-

9 cial intelligence safety incidents.

10 (E) Support the development of norms for

11 reporting of substantial artificial intelligence se-

12 curity incidents and substantial artificial intel-

13 ligence safety incidents, taking into account

14 when it is appropriate to publicly disclose such

15 incidents.

16 (3) REPORT.—Not later than three years after

17 the date of the enactment of this Act, the Director

18 of the National Institute of Standards and Tech-

19 nology shall submit to Congress a report on a proc-

20 ess relating to the voluntary collection, reporting,

21 and tracking of substantial artificial intelligence se-

22 curity incidents and substantial artificial intelligence

23 safety incidents under paragraph (1). Such report

24 shall include the following:

1   (A) Findings from the multi-stakeholder

2   process referred to in such paragraph.

3   (B) An assessment of and recommenda-

4   tions for establishing reporting and collection

5   mechanisms by which industry, academia, non-

6   profit organizations, standards development or-

7   ganizations, civil society groups, and appro-

8   priate public sector entities may voluntarily

9   share standardized information regarding sub-

10   stantial artificial intelligence security incidents

11   and substantial artificial intelligence safety inci-

12   dents;

13   (c) LIMITATION.—Nothing in this section provides

14 the Director of the National Institute of Standards and

15 Technology with any enforcement authority that was not

16 in effect on the day before the date of the enactment of

17 this section.

18   (d) DEFINITIONS.—In this section:

19   (1) ARTIFICIAL INTELLIGENCE.—The term ''ar-

20   tificial intelligence'' has the meaning given such

21   term in section 5002 of the National Artificial Intel-

22   ligence Initiative Act of 2020 (15 U.S.C. 9401).

23   (2) ARTIFICIAL INTELLIGENCE SECURITY VUL-

24   NERABILITY.—The term ''artificial intelligence secu-

25   rity vulnerability'' means a weakness in an artificial

1 intelligence system, system security procedures, in-
2 ternal controls, or implementation that could be ex-
3 ploited or triggered by a threat source.

4 (3) ARTIFICIAL INTELLIGENCE SYSTEM.—The
5 term "artificial intelligence system" has the meaning
6 given such term in section 7223 of the Advancing
7 American AI Act (40 U.S.C. 11301 note; as enacted
8 as part of title LXXII of division G of the James
9 M. Inhofe National Defense Authorization Act for
10 Fiscal Year 2023; Public Law 117–263).

11 (4) SECTOR RISK MANAGEMENT AGENCY.—The
12 term "Sector Risk Management Agency" has the
13 meaning given such term in section 2200 of the
14 Homeland Security Act of 2002 (6 U.S.C. 650).

15 (5) THREAT SOURCE.—The term "threat
16 source" means any of the following:

17 (A) An intent and method targeted at the
18 intentional exploitation of a vulnerability.

19 (B) A situation and method that may acci-
20 dentally trigger a vulnerability.