

.....
(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. _____

To improve the tracking and processing of security and safety incidents and risks associated with artificial intelligence, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To improve the tracking and processing of security and safety incidents and risks associated with artificial intelligence, 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 “Secure Artificial Intel-
5 ligence Act of 2024” or the “Secure A.I. Act of 2024”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) ARTIFICIAL INTELLIGENCE SAFETY INCI-
2 DENT.—The term “artificial intelligence safety inci-
3 dent” means an event that increases the risk that
4 operation of an artificial intelligence system will—

5 (A) result in physical or psychological
6 harm; or

7 (B) lead to a state in which human life,
8 health, or property is endangered.

9 (2) ARTIFICIAL INTELLIGENCE SECURITY INCI-
10 DENT.—The term “artificial intelligence security in-
11 cident” means an event that increases—

12 (A) the risk that operation of an artificial
13 intelligence system occurs in a way that enables
14 the extraction of information about the behavior
15 or characteristics of an artificial intelligence
16 system by a third party; or

17 (B) the ability of a third party to manipu-
18 late an artificial intelligence system in order to
19 subvert the confidentiality, integrity, or avail-
20 ability of an artificial intelligence system or ad-
21 jacent system.

22 (3) ARTIFICIAL INTELLIGENCE SECURITY VUL-
23 NERABILITY.—The term “artificial intelligence secu-
24 rity vulnerability” means a weakness in an artificial
25 intelligence system that could be exploited by a third

1 party to subvert, without authorization, the con-
2 fidentiality, integrity, or availability of an artificial
3 intelligence system, including through techniques
4 such as—

- 5 (A) data poisoning;
- 6 (B) evasion attacks;
- 7 (C) privacy-based attacks; and
- 8 (D) abuse attacks.

9 (4) COUNTER-ARTIFICIAL INTELLIGENCE.—The
10 term “counter-artificial intelligence” means tech-
11 niques or procedures to extract information about
12 the behavior or characteristics of an artificial intel-
13 ligence system, or to learn how to manipulate an ar-
14 tificial intelligence system, in order to subvert the
15 confidentiality, integrity, or availability of an artifi-
16 cial intelligence system or adjacent system.

17 **SEC. 3. VOLUNTARY TRACKING AND PROCESSING OF SECU-**
18 **RITY AND SAFETY INCIDENTS AND RISKS AS-**
19 **SOCIATED WITH ARTIFICIAL INTELLIGENCE.**

20 (a) PROCESSES AND PROCEDURES FOR VULNER-
21 ABILITY MANAGEMENT.—Not later than 180 days after
22 the date of the enactment of this Act, the Director of the
23 National Institute of Standards and Technology shall—

- 24 (1) initiate a process to update processes and
25 procedures associated with the National Vulner-

1 ability Database of the Institute to ensure that the
2 database and associated vulnerability management
3 processes incorporate artificial intelligence security
4 vulnerabilities to the greatest extent practicable; and
5 (2) identify any characteristics of artificial in-
6 telligence security vulnerabilities that make utiliza-
7 tion of the National Vulnerability Database inappro-
8 priate for their management and develop processes
9 and procedures for vulnerability management for
10 those vulnerabilities.

11 (b) VOLUNTARY TRACKING OF ARTIFICIAL INTEL-
12 LIGENCE SECURITY AND ARTIFICIAL INTELLIGENCE
13 SAFETY INCIDENTS.—

14 (1) VOLUNTARY DATABASE REQUIRED.—Not
15 later than 1 year after the date of the enactment of
16 this Act, the Director of the Institute, in coordina-
17 tion with the Director of the Cybersecurity and In-
18 frastructure Security Agency, shall—

19 (A) develop and establish a comprehensive,
20 voluntary database to publicly track artificial
21 intelligence security and artificial intelligence
22 safety incidents; and

23 (B) in establishing the database under sub-
24 paragraph (A)—

1 (i) establish mechanisms by which pri-
2 vate sector entities, public sector organiza-
3 tions, civil society groups, and academic re-
4 searchers, (including current and former
5 employees and contractors of such entities,
6 organizations, and groups), may volun-
7 tarily share information with the Institute
8 on confirmed or suspected artificial intel-
9 ligence security or artificial intelligence
10 safety incidents, in a manner that pre-
11 serves confidentiality of any affected party
12 and of the reporting party;

13 (ii) leverage, to the greatest extent
14 possible, standardized disclosure and inci-
15 dent description formats;

16 (iii) develop processes to associate re-
17 ports pertaining to the same incident with
18 a single incident identifier;

19 (iv) establish classification, informa-
20 tion retrieval, and reporting mechanisms
21 that sufficiently differentiate between arti-
22 ficial intelligence security incidents and ar-
23 tificial intelligence safety incidents; and

1 (v) create appropriate taxonomies to
2 classify incidents based on relevant charac-
3 teristics, impact, or other relevant criteria.

4 (2) IDENTIFICATION AND TREATMENT OF MA-
5 TERIAL ARTIFICIAL INTELLIGENCE SECURITY OR AR-
6 TIFICIAL INTELLIGENCE SAFETY RISKS.—

7 (A) IN GENERAL.—Upon receipt of rel-
8 evant information on an artificial intelligence
9 security or artificial intelligence safety incident,
10 the Director of the Institute shall determine
11 whether the described incident presents a mate-
12 rial artificial intelligence security or artificial
13 intelligence safety risk sufficient for inclusion in
14 the database developed and established under
15 paragraph (1).

16 (B) PRIORITIES.—In evaluating a reported
17 incident pursuant to paragraph (1), the Direc-
18 tor shall prioritize inclusion in the database
19 cases in which a described incident—

20 (i) describes an artificial intelligence
21 system used in critical infrastructure or
22 safety-critical systems;

23 (ii) would result in a high-severity or
24 catastrophic impact to the people or econ-
25 omy of the United States; or

1 (iii) includes an artificial intelligence
2 system widely used in commercial or public
3 sector contexts.

4 (3) REPORTS AND ANONYMITY.—The Director
5 shall populate the voluntary database developed and
6 established under paragraph (1) with incidents
7 based on public reports and information shared
8 using the mechanism established pursuant to sub-
9 paragraph (B)(i) of such paragraph, ensuring that
10 any incident description sufficiently anonymizes
11 those affected, unless those who are affected have
12 consented to their names being included in the data-
13 base.

14 (4) PROTECTION OF REPORTING PARTIES.—

15 (A) PROHIBITION AGAINST RETALIA-
16 TION.—No employer may, directly or indirectly,
17 discharge, demote, suspend, threaten, blacklist,
18 harass, or in any other manner discriminate
19 against any current or former employee or con-
20 tractor in the terms and conditions of employ-
21 ment or postemployment because of any act
22 done by such employee or contractor—

23 (i) in reporting incidents in accord-
24 ance with the mechanisms established in
25 this section;

1 (ii) in reporting incidents to any
2 Member of Congress or any committee of
3 Congress; or

4 (iii) in initiating, testifying in, or as-
5 sisting in any investigation or judicial or
6 administrative action based upon or related
7 to the incidents described in clause (i) or
8 (ii).

9 In addition, no employer may require their em-
10 ployees or contractors to obtain prior consent
11 from such employer to report incidents using
12 the reporting mechanism established in this sec-
13 tion or to any Member of Congress or any com-
14 mittee of Congress, or to obtain prior consent
15 to participate in investigations, judicial, or ad-
16 ministrative actions based upon or related to
17 such incidents.

18 (B) ENFORCEMENT.—Any individual who
19 alleges discharge or other discrimination, or is
20 otherwise aggrieved by an employer or former
21 employer, in violation of subparagraph (A), may
22 seek relief by—

23 (i) filing a complaint with the Sec-
24 retary of Labor in accordance with the re-
25 quirements of this subsection; or

1 (ii) if the Secretary of Labor has not
2 issued a final decision within 180 days of
3 the filing of a complaint under clause (i),
4 and there is no showing that such a delay
5 is due to the bad faith of the claimant,
6 bringing an action against the employer at
7 law or in equity in the appropriate district
8 court of the United States, which shall
9 have jurisdiction over such an action with-
10 out regard to the amount in controversy.

11 (C) CONFIDENTIALITY.—The Director,
12 and any officer or employee of the National In-
13 stitute of Standards and Technology or the Cy-
14 bersecurity and Infrastructure Security Agency,
15 shall not disclose any information, including in-
16 formation provided by a whistleblower to either
17 such official, which could reasonably be ex-
18 pected to reveal the identity of a whistleblower,
19 except in accordance with the provisions of sec-
20 tion 552a of title 5, United States Code, unless
21 and until required to be disclosed to a defend-
22 ant or respondent in connection with a public
23 proceeding instituted by the appropriate such
24 official.

1 (D) RIGHTS RETAINED.—Nothing in this
2 section shall be deemed to diminish the rights,
3 privileges, or remedies of any whistleblower
4 under any Federal or State law or under any
5 collective bargaining agreement.

6 **SEC. 4. UPDATING PROCESSES AND PROCEDURES RELAT-**
7 **ING TO COMMON VULNERABILITIES AND EX-**
8 **POSURES PROGRAM AND EVALUATION OF**
9 **CONSENSUS STANDARDS RELATING TO ARTI-**
10 **FICIAL INTELLIGENCE SECURITY VULNER-**
11 **ABILITY REPORTING.**

12 (a) DEFINITIONS.—In this section:

13 (1) COMMON VULNERABILITIES AND EXPO-
14 SURES PROGRAM.—The term “Common
15 Vulnerabilities and Exposures Program” means the
16 reference guide and classification system for publicly
17 known information security vulnerabilities sponsored
18 by the Cybersecurity and Infrastructure Security
19 Agency.

20 (2) RELEVANT CONGRESSIONAL COMMIT-
21 TEES.—The term “relevant congressional commit-
22 tees” means—

23 (A) the Committee on Homeland Security
24 and Governmental Affairs, the Committee on
25 Commerce, Science, and Transportation, the

1 Select Committee on Intelligence, and the Com-
2 mittee on the Judiciary of the Senate; and

3 (B) the Committee on Oversight and Ac-
4 countability, the Committee on Energy and
5 Commerce, the Permanent Select Committee on
6 Intelligence, and the Committee on the Judici-
7 ary of the House of Representatives.

8 (b) IN GENERAL.—Not later than 180 days after the
9 date of enactment of this Act, the Director of the Cyberse-
10 curity and Infrastructure Security Agency shall—

11 (1) initiate a process to update processes and
12 procedures associated with the Common
13 Vulnerabilities and Exposures Program to ensure
14 that the program and associated processes identify
15 and enumerate artificial intelligence security
16 vulnerabilities to the greatest extent practicable; and

17 (2) identify any characteristic of artificial intel-
18 ligence security vulnerabilities that make utilization
19 of the Common Vulnerabilities and Exposures Pro-
20 gram inappropriate for their management and de-
21 velop processes and procedures for vulnerability
22 identification and enumeration for those artificial in-
23 telligence security vulnerabilities.

24 (c) EVALUATION OF CONSENSUS STANDARDS.—

1 (1) IN GENERAL.—Not later than 30 days after
2 the date of enactment of this Act, the Director of
3 the National Institute of Standards and Technology
4 shall initiate a multi-stakeholder process to evaluate
5 whether existing voluntary consensus standards for
6 vulnerability reporting effectively accommodate arti-
7 ficial intelligence security vulnerabilities.

8 (2) REPORT.—

9 (A) SUBMISSION.—Not later than 180
10 days after the date on which the evaluation
11 under paragraph (1) is carried out, the Director
12 shall submit a report to the relevant congress-
13 sional committees on the sufficiency of existing
14 vulnerability reporting processes and standards
15 to accommodate artificial intelligence security
16 vulnerabilities.

17 (B) POST-REPORT ACTION.—If the Direc-
18 tor concludes in the report submitted under
19 subparagraph (A) that existing processes do not
20 sufficiently accommodate reporting of artificial
21 intelligence security vulnerabilities, the Director
22 shall initiate a process, in consultation with the
23 Director of the National Institute of Standards
24 and Technology and the Director of the Office
25 of Management and Budget, to update relevant

1 vulnerability reporting processes, including the
2 Department of Homeland Security Binding
3 Operational Directive 20–01, or any subsequent
4 directive.

5 (d) BEST PRACTICES.—Not later than 90 days after
6 the date of enactment of this Act, the Director of the Cy-
7 bersecurity and Infrastructure Security Agency shall, in
8 collaboration with the Director of the National Security
9 Agency and the Director of the National Institute of
10 Standards and Technology and by leveraging efforts of the
11 Information Communications Technology Supply Chain
12 Risk Management Task Force to the greatest extent prac-
13 ticable, convene a multi-stakeholder process to encourage
14 the development and adoption of best practices relating
15 to addressing supply chain risks associated with training
16 and maintaining artificial intelligence models, which shall
17 ensure consideration of supply chain risks associated
18 with—

19 (1) data collection, cleaning, and labeling, par-
20 ticularly the supply chain risks of reliance on remote
21 workforce and foreign labor for such tasks;

22 (2) inadequate documentation of training data
23 and test data storage, as well as limited provenance
24 of training data;

1 (b) FUNCTIONS.—The functions of the Artificial In-
2 telligence Security Center shall be as follows:

3 (1) Making available a research test-bed to pri-
4 vate sector and academic researchers, on a sub-
5 sidized basis, to engage in artificial intelligence secu-
6 rity research, including through the secure provision
7 of access in a secure environment to proprietary
8 third-party models with the consent of the vendors
9 of the models.

10 (2) Developing guidance to prevent or mitigate
11 counter-artificial intelligence techniques.

12 (3) Promoting secure artificial intelligence
13 adoption practices for managers of national security
14 systems (as defined in section 3552 of title 44,
15 United States Code) and elements of the defense in-
16 dustrial base.

17 (4) Coordinating with the Artificial Intelligence
18 Safety Institute within the National Institute of
19 Standards and Technology.

20 (5) Such other functions as the Director con-
21 siders appropriate.

22 (c) TEST-BED REQUIREMENTS.—

23 (1) ACCESS AND TERMS OF USAGE.—

24 (A) RESEARCHER ACCESS.—The Director
25 shall establish terms of usage governing re-

1 searcher access to the test-bed made available
2 under subsection (b)(1), with limitations on re-
3 searcher publication only to the extent nec-
4 essary to protect classified information or pro-
5 prietary information concerning third-party
6 models provided through the consent of model
7 vendors.

8 (B) AVAILABILITY TO FEDERAL AGEN-
9 CIES.—The Director shall ensure that the test-
10 bed made available under subsection (b)(1) is
11 also made available to other Federal agencies
12 on a cost-recovery basis.

13 (2) USE OF CERTAIN INFRASTRUCTURE AND
14 OTHER RESOURCES.—In carrying out subsection
15 (b)(1), the Director shall leverage, to the greatest
16 extent practicable, infrastructure and other re-
17 sources provided under section 5.2 of the Executive
18 Order dated October 30, 2023 (relating to safe, se-
19 cure, and trustworthy development and use of artifi-
20 cial intelligence).

21 (d) ACCESS TO PROPRIETARY MODELS.—In carrying
22 out this section, The Director shall establish such mecha-
23 nisms as the Director considers appropriate, including po-
24 tential contractual incentives, to ensure the provision of
25 access to proprietary models by qualified independent,

- 1 third-party researchers, provided that commercial model
- 2 vendors have voluntarily provided models and associated
- 3 resources for such testing.