

119TH CONGRESS
2D SESSION

S. _____

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

IN THE SENATE OF THE UNITED STATES

Mr. WARNER introduced the following bill; which was read twice and 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 Development Act of 2026” or the “Secure A.I. De-
6 velopment Act of 2026”.

7 **SEC. 2. DEFINITIONS.**

8 In this Act:

9 (1) ADVERSARIAL-ARTIFICIAL INTEL-
10 LIGENCE.—The term “adversarial-artificial intel-

1 ligence” means techniques or procedures to extract
2 information about the behavior or characteristics of
3 an artificial intelligence system, or to learn how to
4 manipulate an artificial intelligence system, in order
5 to subvert the confidentiality, integrity, or avail-
6 ability of an artificial intelligence system or adjacent
7 system.

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

12 (3) ARTIFICIAL INTELLIGENCE SAFETY INCI-
13 DENT.—The term “artificial intelligence safety inci-
14 dent” means an event that materially increases the
15 risk that operation of an artificial intelligence sys-
16 tem leads to a state in which human life, health,
17 property, or the environment is endangered.

18 (4) ARTIFICIAL INTELLIGENCE SECURITY INCI-
19 DENT.—The term “artificial intelligence security in-
20 cident” means an event that materially increases—

21 (A) the risk that operation of an artificial
22 intelligence system occurs in a way that enables
23 the unauthorized extraction of information
24 about the behavior or characteristics of an arti-

1 ficial intelligence system by an unauthorized
2 party; or

3 (B) the ability to manipulate an artificial
4 intelligence system in order to subvert the con-
5 fidentiality, integrity, or availability of an artifi-
6 cial intelligence system or adjacent system.

7 (5) ARTIFICIAL INTELLIGENCE SECURITY VUL-
8 NERABILITY.—The term “artificial intelligence secu-
9 rity vulnerability” means a weakness in an artificial
10 intelligence system that could be exploited by a third
11 party to subvert, without authorization, the con-
12 fidentiality, integrity, or availability of an artificial
13 intelligence system, including through techniques
14 such as—

15 (A) data poisoning;

16 (B) evasion attacks;

17 (C) privacy-based attacks;

18 (D) model theft or extraction attacks;

19 (E) attacks designed to circumvent or de-
20 grade the safety, alignment, or access control
21 mechanisms of an artificial intelligence system;
22 and

23 (F) adversarial machine learning attacks
24 as described in National Institute of Standards
25 and Technology Trustworthy and Responsible

1 Artificial Intelligence 100–2e2025 (relating to
2 Adversarial Machine Learning), or successor
3 publication.

4 **SEC. 3. ENABLING TESTING OF FRONTIER ARTIFICIAL IN-**
5 **TELLIGENCE MODELS PRIOR TO PUBLIC RE-**
6 **LEASE.**

7 (a) DEFINITIONS.—In this section:

8 (1) BOARD.—The term “Board” means the Ar-
9 tificial Intelligence Risk Board established under
10 subsection (b)(1).

11 (2) CRITICAL INFRASTRUCTURE.—The term
12 “critical infrastructure” has the meaning provided in
13 section 1016(e) of the USA Patriot Act of 2001 (42
14 U.S.C. 5195c(e)).

15 (3) FRONTIER ARTIFICIAL INTELLIGENCE
16 MODEL.—The term “frontier artificial intelligence
17 model” means an artificial intelligence model, or sys-
18 tem combining multiple artificial intelligence models,
19 that exhibits or could be modified to exhibit high lev-
20 els of performance at tasks that pose a serious risk
21 to national security, national economic security, or
22 public health or safety.

23 (4) INSTITUTE.—The term “Institute” means
24 the National Institute of Standards and Technology.

1 (5) SECRETARY.—The term “Secretary” means
2 the Secretary of Commerce.

3 (b) THE ARTIFICIAL INTELLIGENCE RISK BOARD.—

4 (1) ESTABLISHMENT.—

5 (A) IN GENERAL.—Not later than 90 days
6 after the date of the enactment of this Act, the
7 Secretary shall establish within the Institute a
8 board to address artificial intelligence risks.

9 (B) DESIGNATION.—The board established
10 under subparagraph (A) shall be known as the
11 “Artificial Intelligence Risk Board”.

12 (2) MEMBERSHIP.—

13 (A) COMPOSITION.—The Board shall be
14 composed of members who are appointed as fol-
15 lows:

16 (i) One of more members selected by
17 the Director of the National Institute of
18 Standards.

19 (ii) One of more members selected by
20 the Secretary.

21 (iii) One of more members selected by
22 the Director of the Cybersecurity and In-
23 frastructure Security Agency.

1 (iv) One of more members selected by
2 the Director of the National Security
3 Agency.

4 (v) One of more members selected by
5 the Secretary of the Treasury.

6 (B) NONGOVERNMENTAL EXPERTS.—In
7 addition to the members of the Board appointed
8 under subparagraph (A), the Secretary shall ap-
9 point members who are not officers or employ-
10 ees of the Federal Government and who the
11 Secretary selects from among individuals who—

12 (i) are leading technical experts not
13 affiliated with a developer or provider of
14 artificial intelligence systems;

15 (ii) are leading technical experts affili-
16 ated with developers or providers of artifi-
17 cial intelligence systems;

18 (iii) are individuals with expertise in
19 developing evaluations to test artificial in-
20 telligence models; and

21 (iv) have knowledge or expertise that
22 the Secretary determines would further the
23 purpose of the duties of the Board.

24 (3) TERMS AND VACANCIES.—

1 (A) TERMS.—Each member of the Board
2 shall serve 1 term of not longer than 3 years
3 and may be reappointed for 1 successive term
4 of not longer than 3 years.

5 (B) VACANCY REPLACEMENT.—The
6 memebtrs of the Board shall develop a vacancy
7 replacement procedure that includes—

8 (i) for vacancies occurring due to the
9 end of a member's term, a vote not later
10 than 90 days before the last day of the
11 member's term; and

12 (ii) for vacancies occurring under sub-
13 paragraph (C) or for any other reason, the
14 chair of the Board shall nominate a re-
15 placement from the same stakeholder cat-
16 egory under paragraph (2), to the extent
17 practicable, as the member creating the va-
18 cancy, subject to approval by a majority
19 vote of the members of the Board.

20 (C) REMOVAL.—Any member who fails to
21 comply with the conflict of interest policy
22 adopted pursuant to paragraph (5)(D) shall be
23 removed from the Board.

24 (D) CHAIR.—The chair of the Board shall
25 be selected by a majority vote among a quorum

1 of the members appointed under paragraph (2)
2 and shall serve not more than 1 two-year term.

3 (4) MEMBER ACCESS TO CLASSIFIED INFORMA-
4 TION.—

5 (A) ACCESS.—

6 (i) IN GENERAL.—Not later than 60
7 days after the date on which a member is
8 first appointed to the Board and before the
9 member is granted access to any classified
10 information necessary to participate in a
11 closed session pursuant to paragraph
12 (5)(F), the Secretary shall determine, for
13 the purposes of the Board, if the member
14 should be restricted from reviewing, dis-
15 cussing, or possessing classified informa-
16 tion.

17 (ii) MANAGEMENT.—Access to classi-
18 fied information shall be managed in ac-
19 cordance with Executive Order 13526 (50
20 U.S.C. 3161 note; relating to classified na-
21 tional security information), or any subse-
22 quent corresponding Executive Order.

23 (iii) CLEARANCE REQUIREMENT.—
24 The Secretary shall sponsor each member
25 of the Board for a security clearance at the

1 Top Secret level with access to sensitive
2 compartmented information, as appro-
3 priate, for the purposes of participating in
4 carrying out the duties of the Board.

5 (iv) CLEARANCE REQUIREMENT.—

6 Each member of the Board shall obtain a
7 security clearance unless denied by the ap-
8 propriate authorities or if the Secretary de-
9 termines a member should be restricted
10 from reviewing, discussing, or possessing
11 classified information. In either instance,
12 such member shall be removed from the
13 Board and a new member shall be ap-
14 pointed pursuant to the vacancy proce-
15 dures under paragraph (3)(B) to replace
16 such removed member.

17 (B) PROTECTION OF INFORMATION.—A

18 member of the Board granted access to classi-
19 fied information shall protect the classified in-
20 formation in accordance with the applicable re-
21 quirements for the particular level of classifica-
22 tion of the information.

23 (C) RULE OF CONSTRUCTION.—Nothing in
24 this paragraph shall be construed to affect the
25 existing security clearance of a member of the

1 Board or the authority of a Federal agency to
2 provide or deny a member of the Board access
3 to any specific pieces of classified information.

4 (5) PROCEDURES.—

5 (A) DESIGNATED FEDERAL OFFICER.—

6 The Secretary shall designate a Federal officer
7 or employee to serve as the designated federal
8 officer of the Board, consistent with the re-
9 quirements of chapter 10 of title 5, United
10 States Code (common known as the “Federal
11 Advisory Committee Act”).

12 (B) INITIAL MEETING AND BYLAWS.—Not
13 later than 120 days after the date of the enact-
14 ment of this Act, the Board shall convene and
15 establish bylaws that—

16 (i) govern quorum and voting rules,
17 including implementation of the decision-
18 making majority voting requirement speci-
19 fied in paragraph (5)(C)(ii); and

20 (ii) set deliverable timelines and meet-
21 ing schedules.

22 (C) OPERATING PROCEDURES.—Unless
23 otherwise specified, the Board shall adopt writ-
24 ten procedures governing its meetings, con-

sistent with chapter 10 of title 5, United States Code, that include—

(i) requirements for public notice of meetings and the maintenance of records and minutes;

(ii) decision making by majority vote
of those present and voting;

(iii) authorization for the establishment of subgroups as necessary, subject to the approval of the chair of the Board; and

(iv) approval of the meeting agendas by the chair in consultation with the designated federal officer under subparagraph (A) to ensure compliance with applicable laws.

(D) CONFLICT-OF-INTEREST POLICY.—

(i) IN GENERAL.—The Board shall adopt and enforce a written conflict of interest policy to ensure that members of the Board have a fiduciary responsibility to the Board, a duty to report conflicts of interest, including the appearance of a conflict of interest, and do not participate in deliberations or votes from which they person-

1 ally or their employer would directly and
2 materially benefit.

3 (ii) REQUIRED DISCLOSURES.—The
4 policy under clause (i) shall require each
5 member to publicly disclose all relevant fi-
6 nancial and employment relationships and
7 include recusal procedures in the event of
8 a conflict.

9 (iii) RECORDS.—The designated fed-
10 eral officer under subparagraph (A) shall
11 maintain records of disclosures under
12 clause (ii) of this subparagraph and make
13 summaries of the disclosures available to
14 the Secretary.

15 (E) THREAT INFORMATION ACCESS.—The
16 Director of National Intelligence, in coordina-
17 tion with the heads of other appropriate Fed-
18 eral entities, shall ensure that the Board has
19 access to relevant cybersecurity threat informa-
20 tion, including through closed or classified
21 briefings or the provision of classified informa-
22 tion, when appropriate.

23 (F) CLOSED SESSIONS.—Notwithstanding
24 section 1009 of title 5, United States Code, the
25 Board may hold closed or restricted-access ses-

sions when the Secretary determines that the matters to be discussed involve any of the following:

(i) Classified information.

(ii) Sensitive cybersecurity vulnerabilities.

(iii) Threat information.

(iv) Proprietary business information.

(v) Other information exempt from public disclosure under section 552 of title 5, United States Code.

(6) DUTIES.—

(A) IN GENERAL.—The Board shall—

(i) develop a process to perform technical evaluations to determine what capabilities or combination of capabilities constitute high levels of performance at tasks that pose a serious risk to national security, national economic security, or public health or safety; and

(ii) develop best practices, including—

(I) standardize formats and processes for publishing model cards with technical details of artificial intelligence systems;

1 (II) recommendations for main-
2 taining cybersecurity measures for de-
3 velopers or providers of artificial intel-
4 ligence systems;

5 (III) processes and metrics for
6 developers or providers of artificial in-
7 telligence systems to use to evaluate
8 risks from employees or other per-
9 sonnel who have access to artificial in-
10 telligence systems developed or in de-
11 velopment by developers or providers
12 of artificial intelligence systems; and

13 (IV) recommendations on appro-
14 priate financial and other resourcing
15 for developers or providers of artificial
16 intelligence systems to robustly en-
17 gage in safety and security research
18 focused on the deployment of frontier
19 artificial intelligence models.

20 (B) PERIODIC REASSESSMENT OF TECH-
21 NICAL EVALUATIONS AND BEST PRACTICES.—
22 The Board shall periodically reassess the tech-
23 nical evaluations and best practices the Board
24 develops under this subsection.

1 (c) REQUIREMENT THAT PROVIDERS OF FRONTIER
2 ARTIFICIAL INTELLIGENCE MODELS GIVE ACCESS TO
3 NATIONAL SECURITY AGENCY BEFORE PUBLIC RE-
4 LEASE.—Not later than 21 calendar days before a pro-
5 vider introduces into interstate or foreign commerce a
6 frontier artificial intelligence model, the provider shall
7 make available to the Artificial Intelligence Security Cen-
8 ter, established by the Director of the National Security
9 Agency under section 6504 of the Intelligence Authoriza-
10 tion Act for Fiscal Year 2025 (division F of Public Law
11 118–159; 50 U.S.C. 3602 note), access to the frontier ar-
12 tificial intelligence model, including model’s weights, con-
13 figuration files, runtimes, or software libraries necessary
14 to operate the frontier artificial intelligence model.

15 (d) FRONTIER ARTIFICIAL INTELLIGENCE MODEL
16 REGISTRY.—

17 (1) ESTABLISHMENT OF REGISTRY.—Not later
18 than 90 days after the date of the enactment of this
19 Act, the Director of the National Institute of Stand-
20 ards and Technology shall establish a registry of
21 frontier models that are available to the public.

22 (2) RULES AND PROCEDURES.—In establishing
23 the registry under paragraph (1), the Director of the
24 National Institute of Standards and Technology
25 shall establish rules and procedures for—

1 (A) a provider of a frontier artificial intel-
2 ligence model to register the frontier artificial
3 intelligence model;

4 (B) a provider of a frontier artificial intel-
5 ligence model to contest the need for registering
6 the frontier artificial intelligence model;

7 (C) removing a frontier artificial intel-
8 ligence model from the registry;

9 (D) a provider of a frontier artificial intel-
10 ligence model to attest that the provider sub-
11 mitted the frontier artificial intelligence model
12 to the test-bed established under section
13 6504(e) of the Intelligence Authorization Act
14 for Fiscal Year 2025 (division F of Public Law
15 118–159; 50 U.S.C. 3602 note), as amended by
16 subsection (e); and

17 (E) such other purposes the Director
18 deems necessary.

19 (3) OBLIGATION TO REGISTER.—Each provider
20 of a frontier artificial intelligence model shall reg-
21 ister that frontier artificial intelligence model with
22 the registry established under paragraph (1) before
23 introducing the frontier artificial intelligence model
24 into interstate or foreign commerce.

25 (e) ENFORCEMENT; ABILITY TO CURE.—

1 (1) REFERRALS FOR ENFORCEMENT.—In any
2 case in which the Director of the National Institute
3 of Standards and Technology determines that a
4 frontier artificial intelligence model has been intro-
5 duced into interstate or foreign commerce by a pro-
6 vider of the frontier artificial intelligence in violation
7 of subsection (c), the Director of the National Insti-
8 tute of Standards and Technology shall notify the
9 Attorney General.

10 (2) ENFORCEMENT.—The Attorney General
11 shall enforce this section.

12 (3) PENALTY.—Whoever violates subsection (c)
13 shall be fined an amount equal to not less than
14 \$100,000 per day for each day during which a fron-
15 tier artificial intelligence model controlled by that
16 person is available through interstate and foreign
17 commerce without having obtained the voluntary se-
18 curity guidance issued under section 6504(e)(3) of
19 the Intelligence Authorization Act for Fiscal Year
20 2025 (division F of Public Law 118–159; 50 U.S.C.
21 3602 note), as amended by subsection (f).

22 (4) RIGHT TO CURE.—

23 (A) NOTIFICATION.—Prior to commencing
24 an enforcement action against a provider of a
25 frontier artificial intelligence model for violating

1 subsection (c), the Attorney General shall notify
2 the provider and allow the provider 7 calendar
3 days following the notice of violation for the vio-
4 lator to come into compliance pursuant to sub-
5 paragraph (B).

6 (B) PROCESS TO CURE.—In order for a
7 provider of a frontier artificial intelligence
8 model to come into compliance pursuant to this
9 subparagraph, the provider shall demonstrate to
10 the Attorney General that the provider has—

11 (i) withdrawn from interstate and for-
12 eign commerce the frontier artificial intel-
13 ligenge model that gave rise to the viola-
14 tion of subsection (c); and

15 (ii) given to the National Security
16 Agency access to the frontier artificial in-
17 telligenge model pursuant to subsection (c).

18 (f) NATIONAL SECURITY AGENCY RESEARCH-TEST-
19 BED.—Section 6504 of the Intelligence Authorization Act
20 for Fiscal Year 2025 (division F of Public Law 118–159;
21 50 U.S.C. 3602 note) is amended—

22 (1) in subsection (c)—

23 (A) by redesignating paragraph (4) as
24 paragraph (5); and

1 (B) by inserting after paragraph (3) the
2 following new paragraph (4):

3 “(3) Making available a research test-bed to
4 private sector, Federal and qualified independent ex-
5 pert participants, on a subsidized basis, to engage in
6 artificial intelligence security research, including
7 through the secure provision of access in a secure
8 environment for pre-deployment testing of any fron-
9 tier artificial intelligence model prior to public re-
10 lease.”;

11 (2) by redesignating subsection (e) as sub-
12 section (f); and

13 (3) by inserting after subsection (d) the fol-
14 lowing:

15 “(e) TEST-BED REQUIREMENTS.—

16 “(1) ACCESS AND TERMS OF USAGE.—

17 “(A) OUTSIDE PARTICIPATION.—The Di-
18 rector shall establish a process by which critical
19 infrastructure operators, as well private sector
20 entities that develop or maintain information
21 systems utilized by critical infrastructure opera-
22 tors, shall access a secure test-bed for the pur-
23 pose of testing and evaluating the impact of
24 frontier artificial intelligence models on infor-
25 mation systems maintained by critical infra-

1 structure operators prior to public release or
2 distribution of such models.

3 “(B) RESEARCHER ACCESS.—The Director
4 shall establish terms of usage governing access
5 to the test-bed made available under subsection
6 (c)(4), with limitations on researcher publica-
7 tion to the extent necessary to protect classified
8 information or proprietary information provided
9 by private sector participants.

10 “(C) AVAILABILITY TO FEDERAL AGEN-
11 CIES.—The Director shall ensure that the test-
12 bed made available under subsection (c)(4) is
13 also made available to other Federal agencies
14 on a cost-recovery basis.

15 “(2) USE OF CERTAIN INFRASTRUCTURE AND
16 OTHER RESOURCES.—In carrying out subsection
17 (c)(4), the Director shall leverage, to the greatest ex-
18 tent practicable, infrastructure and other resources
19 provided under section 5.2 of Executive Order
20 14110 (88 Fed. Reg. 75191; relating to safe, secure,
21 and trustworthy development and use of artificial in-
22 telligence).

23 “(3) VOLUNTARY SECURITY GUIDANCE.—The
24 Director shall share relevant guidance, informed by
25 pre-deployment testing in the secure test-bed envi-

1 ronment identified in subsection (c), to inform vol-
2 untary vendor actions to mitigate against potential
3 security threats to such models, or the ability of for-
4 eign actors to utilize such models for computer net-
5 work exploitation campaigns against information
6 systems utilized by critical infrastructure operators,
7 the design or development of weapons systems, or to
8 further foreign surveillance capabilities.”.

9 **SEC. 4. DATABASE FOR ARTIFICIAL INTELLIGENCE SECU-**
10 **RITY AND SAFETY INCIDENTS AND RISKS.**

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

14 (1) VOLUNTARY SUBMISSIONS.—Not later than
15 1 year after the date of the enactment of this Act,
16 the Director of the National Institute of Standards
17 and Technology shall, in coordination with the Di-
18 rector of the Cybersecurity and Infrastructure Secu-
19 rity Agency, establish mechanisms by which private
20 sector entities, public sector organizations, civil soci-
21 ety groups, and academic researchers may volun-
22 tarily share information with the National Institute
23 of Standards and Technology on confirmed or sus-
24 pected artificial intelligence security or artificial in-
25 telligence safety incidents, in a manner that pre-

1 serves confidentiality of any affected party, which
2 shall—

3 (A) leverage, to the greatest extent pos-
4 sible, standardized disclosure and incident de-
5 scription formats;

6 (B) develop processes to associate reports
7 pertaining to the same incident with a single in-
8 cident identifier;

9 (C) establish classification, information re-
10 trieval, and reporting mechanisms that suffi-
11 ciently differentiate between artificial intel-
12 ligence security incidents and artificial intel-
13 ligence safety incidents; and

14 (D) create appropriate taxonomies to clas-
15 sify incidents based on relevant characteristics,
16 impact, or other relevant criteria.

17 (2) PUBLICLY ACCESSIBLE DATABASE.—

18 (A) ESTABLISHMENT OF DATABASE RE-
19 QUIRED.—Not later than 1 year after the date
20 of the enactment of this Act, the Director of
21 the Institute shall, in coordination with the Di-
22 rector of the Cybersecurity and Infrastructure
23 Security Agency, establish a publicly accessible
24 database of artificial intelligence security inci-
25 dents and artificial intelligence safety incidents.

1 (B) REVIEW AND POPULATION OF DATA-
2 BASE.—Upon receipt of relevant information on
3 an artificial intelligence security or artificial in-
4 telligence safety incident under paragraph (1),
5 the Director of the Institute shall review the in-
6 formation and determine whether the described
7 incident constitutes an artificial intelligence se-
8 curity or artificial intelligence safety risk appro-
9 priate for inclusion in the database developed
10 and established under subparagraph (A).

11 (C) IDENTIFICATION OF CAUSAL FAC-
12 TORS.—When making a determination under
13 subparagraph (B), the Director of the Institute
14 shall identify causal factors for the artificial in-
15 telligence security incident or the artificial intel-
16 ligence safety incident, including—

- 17 (i) the artificial intelligence system;
18 (ii) the deployment of the artificial in-
19 telligence systems; and
20 (iii) practices related to the operation
21 of the artificial intelligence system, includ-
22 ing misuse of the artificial intelligence sys-
23 tem.

24 (D) PRIORITIES.—In evaluating informa-
25 tion under subparagraph (B) and determining

1 under such subparagraph whether to include a
2 report of an incident in the database required
3 by subparagraph (A), the Director shall
4 prioritize inclusion in the database of cases in
5 which a described incident—

6 (i) describes an artificial intelligence
7 system used in critical infrastructure or
8 safety-critical systems;

9 (ii) would result in a high-severity or
10 catastrophic impact to the people or econ-
11 omy of the United States; or

12 (iii) includes an artificial intelligence
13 system widely used in commercial or public
14 sector contexts in the United States.

15 (3) EXEMPTION FROM DISCLOSURE; REPORTS
16 AND ANONYMITY.—

17 (A) ANONYMITY.—The Director shall pop-
18 ulate the voluntary database developed and es-
19 tablished under paragraph (2)(A) with incidents
20 based on public reports and information shared
21 using the mechanism established pursuant to
22 paragraph (1), ensuring that any incident de-
23 scription sufficiently anonymizes those affected,
24 unless those who are affected have consented to
25 their names being included in the database.

1 (B) EXEMPTION FROM DISCLOSURE.—Any
2 information shared using the mechanism estab-
3 lished pursuant to paragraph (1)—

4 (i) shall be exempt from disclosure
5 and withheld, unless an affected party con-
6 sents to the inclusion of their names in the
7 database as provided for under subpara-
8 graph (A), from the public, pursuant to
9 section 552(b)(3)(B) of title 5, United
10 States Code, and any other provision of
11 United States law or law of any State, po-
12 litical subdivision or agency thereof, or
13 Tribe requiring disclosure of information
14 or records; and

15 (ii) shall not be deemed a waiver of
16 any applicable privilege or protection, in-
17 cluding trade secret protection.

18 (C) CONSULTATION REQUIRED.—Before
19 publishing information regarding artificial intel-
20 ligence safety incident under paragraph (2)(B),
21 the Director shall consult with the developer or
22 provider of the artificial intelligence system in-
23 volved in an incident.

24 (b) MATERIAL RISK GUIDANCE.—Not later than 180
25 days after the date of the enactment of this Act the Direc-

1 tor of the National Institute of Standards and Technology
2 shall, in coordination with the Director of the Cybersecu-
3 rity and Infrastructure Security Agency, publish non-
4 binding guidance that provides illustrative criteria and ex-
5 amples for determining when an event “materially in-
6 creases” a risk for purposes of paragraphs (3) and (4)
7 of section 2.

8 **SEC. 5. UPDATING PROCESSES AND PROCEDURES RELAT-**
9 **ING TO CYBERSECURITY VULNERABILITIES.**

10 (a) DEFINITIONS.—In this section:

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

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

21 (A) the Committee on Homeland Security
22 and Governmental Affairs, the Committee on
23 Commerce, Science, and Transportation, the
24 Select Committee on Intelligence, and the Com-
25 mittee on the Judiciary of the Senate; and

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

6 (b) PROCESSES AND PROCEDURES FOR VULNER-
7 ABILITY MANAGEMENT.—Not later than 180 days after
8 the date of the enactment of this Act, the Director of the
9 National Institute of Standards and Technology shall—

10 (1) comprehensively evaluate, and develop a
11 strategic plan to reform, the structure and processes
12 of the National Vulnerability Database in light of
13 significant increase in the volume of vulnerabilities
14 in information systems identified by artificial intel-
15 ligence systems, including recommendations and
16 guidance related to assisting in determining
17 prioritization of identified vulnerability patching and
18 mitigation;

19 (2) initiate a process to utilize advanced artifi-
20 cial intelligence systems to characterize
21 vulnerabilities as part of the National Vulnerability
22 Database;

23 (3) initiate a process to update processes and
24 procedures associated with the National Vulner-
25 ability Database of the Institute to ensure that the

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

4 (4) identify any characteristics of artificial in-
5 telligence security vulnerabilities that make utiliza-
6 tion of the National Vulnerability Database inappro-
7 priate and develop processes and procedures for vul-
8 nerability management for those vulnerabilities; and

9 (5) initiate a process to update the Secure Soft-
10 ware Development Framework set forth in National
11 Institute of Standards and Technology Special Pub-
12 lication 800–218 and include guidance and best
13 practices for using artificial intelligence in code gen-
14 eration and security review.

15 (c) UPDATES TO COMMON VULNERABILITIES AND
16 EXPOSURES PROGRAM.—Not later than 180 days after
17 the date of enactment of this Act, the Director of the Cy-
18 bersecurity and Infrastructure Security Agency shall—

19 (1) initiate a process to update processes and
20 procedures associated with the Common
21 Vulnerabilities and Exposures Program to ensure
22 that the program and associated processes identify
23 and enumerate artificial intelligence security
24 vulnerabilities to the greatest extent practicable; and

1 (2) identify any characteristic of artificial intel-
2 ligence security vulnerabilities that make utilization
3 of the Common Vulnerabilities and Exposures Pro-
4 gram inappropriate and develop processes and proce-
5 dures for vulnerability identification and enumera-
6 tion for those artificial intelligence security
7 vulnerabilities.

8 (d) SUBMISSION TO CONGRESS.—Upon completion of
9 the processes required in subsections (a) and (b), the Di-
10 rector of the National Institute of Standards and Tech-
11 nology and the Director of the Cybersecurity and Infra-
12 structure Security Agency, respectively, shall submit a
13 strategic plan to Congress identifying courses of action
14 under existing authorities, or identifying specific legisla-
15 tive amendments, necessary to address accelerating secu-
16 rity risks associated with artificial intelligence systems.

17 (e) EVALUATION OF CONSENSUS STANDARDS FOR
18 VULNERABILITY DISCLOSURE.—

19 (1) IN GENERAL.—Not later than 30 days after
20 the date of the enactment of this Act, the Director
21 of the National Institute of Standards and Tech-
22 nology shall, in coordination with the Director of the
23 Cybersecurity and Infrastructure Security Agency,
24 initiate a multi-stakeholder process to evaluate
25 whether existing voluntary consensus standards and

1 processes for vulnerability reporting processes asso-
2 ciated with the security of information systems effec-
3 tively accommodate the significant increased volume
4 of vulnerabilities in information systems identified
5 by artificial intelligence systems, as well as the
6 unique nature of artificial intelligence security
7 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 congres-
13 sional committees on the sufficiency of existing
14 vulnerability reporting processes and standards
15 to accommodate the significant increased vol-
16 ume of vulnerabilities in information systems
17 identified by artificial intelligence systems, as
18 well as artificial intelligence security
19 vulnerabilities.

20 (B) POST-REPORT ACTION.—If the Direc-
21 tor concludes in the report submitted under
22 subparagraph (A) that existing vulnerability re-
23 porting processes and standards do not effec-
24 tively accommodate the significant increased
25 volume of vulnerabilities in information systems

1 identified by artificial intelligence systems, as
2 well as the reporting of artificial intelligence se-
3 curity vulnerabilities, the Director shall initiate
4 a process, in consultation with the Director of
5 the National Institute of Standards and Tech-
6 nology and the Director of the Office of Man-
7 agement and Budget, to update relevant vulner-
8 ability reporting processes, including the De-
9 partment of Homeland Security Binding Oper-
10 ational Directive 20–01, or any subsequent di-
11 rective.

12 **SEC. 6. REVIEW OF ARTIFICIAL INTELLIGENCE SECURITY**
13 **VULNERABILITIES UNDER VULNERABILITIES**
14 **EQUITIES PROCESS.**

15 (a) DEFINITIONS.—In this section:

16 (1) APPROPRIATE CONGRESSIONAL COMMIT-
17 TEES.—The term “appropriate congressional com-
18 mittees” means—

19 (A) the Select Committee on Intelligence of
20 the Senate;

21 (B) the Committee on Homeland Security
22 and Governmental Affairs of the Senate;

23 (C) the Committee on the Judiciary of the
24 Senate;

1 (D) the Committee on Armed Services of
2 the Senate;

3 (E) the Permanent Select Committee on
4 Intelligence of the House of Representatives;

5 (F) the Committee on Homeland Security
6 of Representatives;

7 (G) the Committee on the Judiciary of the
8 House of Representatives; and

9 (H) the Committee on Armed Services of
10 the House of Representatives.

11 (2) VULNERABILITIES EQUITIES POLICY AND
12 PROCESS DOCUMENT.—The term “Vulnerabilities
13 Equities Policy and Process document” means the
14 executive branch document entitled “Vulnerabilities
15 Equities Policy and Process for the United States
16 Government” dated November 15, 2017.

17 (3) VULNERABILITIES EQUITIES PROCESS.—
18 The term “Vulnerabilities Equities Process” means
19 the interagency review of vulnerabilities carried out
20 pursuant to the Vulnerabilities Equities Policy and
21 Process document or any successor document.

22 (b) EVALUATION; REPORT.—Not later than 90 days
23 after the date of the enactment of this Act, the Federal
24 departments and agencies participating in the
25 Vulnerabilities Equities Process shall—

1 (1) evaluate whether the existing Vulnerabilities
2 Equities Process sufficiently accommodates the sub-
3 mission and review of artificial intelligence security
4 vulnerabilities; and

5 (2) submit to the appropriate congressional
6 committees a report describing the applicability of
7 the Vulnerabilities Equities Process to such
8 vulnerabilities, including whether the submission and
9 review of such vulnerabilities under the
10 Vulnerabilities Equities Process would result in an
11 unduly large volume of notifications to affected ven-
12 dors and, if so, an assessment of mechanisms to
13 manage the volume of such notifications.

14 (c) PROCESS.—In carrying out subsection (b), if the
15 Federal departments and agencies participating in the
16 Vulnerabilities Equities Process determine that the exist-
17 ing Vulnerabilities Equities Process does not sufficiently
18 accommodate the submission and review of artificial intel-
19 ligence security vulnerabilities identified by the evaluation
20 required in subsection (b)(1), and that such vulnerabilities
21 present public interest considerations meriting review
22 under the Vulnerabilities Equities Process, the Federal de-
23 partments and agencies participating in the Vulnerabilities
24 Equities Process shall establish a process for the submis-
25 sion and review of such vulnerabilities under the

1 Vulnerabilities Equities Process not later than 30 days
2 after the date of such determination.

3 (d) REPORT ON VULNERABILITIES IDENTIFIED BY
4 ARTIFICIAL INTELLIGENCE SYSTEMS.—Not later than 90
5 days after the date of the enactment of this Act, the Direc-
6 tor of National Intelligence shall submit to the congres-
7 sional intelligence committees (as defined in section 3 of
8 the National Security Act of 1947 (50 U.S.C. 3003)) a
9 report on—

10 (1) the volume of vulnerabilities of information
11 systems identified by artificial intelligence systems;

12 (2) the impact of any change in such volume on
13 the functioning of the Vulnerabilities Equities Proc-
14 ess; and

15 (3) whether the increasingly rapid discovery
16 and exploitation of such vulnerabilities by external
17 cyber actors using artificial intelligence systems ma-
18 terially alters the equity of disclosure.

19 **SEC. 7. SECURITY OF ARTIFICIAL INTELLIGENCE SYSTEMS**
20 **AND LABORATORIES.**

21 (a) DEFINITIONS.—In this section:

22 (1) CENTER.—The term “Center” means the
23 Artificial Intelligence Security Center of the Na-
24 tional Security Agency.

1 (2) CLASSIFIED INFORMATION.—The term
2 “classified information” has the meaning given such
3 term in section 805 of the National Security Act of
4 1947 (50 U.S.C. 3164).

5 (3) CLEARED INDUSTRY PERSONNEL.—The
6 term “cleared industry personnel” means employees
7 or representatives of a covered person who hold an
8 appropriate security clearance and have a dem-
9 onstrated need to know.

10 (4) CONGRESSIONAL INTELLIGENCE COMMIT-
11 TEES.—The term “congressional intelligence com-
12 mittees” has the meaning given such term in section
13 3 of the National Security Act of 1947 (50 U.S.C.
14 3003).

15 (5) COVERED PERSON.—The term “covered
16 person” means a non-Federal person who—

17 (A) is a United States person;

18 (B) develops, deploys, or operates artificial
19 intelligence models or critical enabling infra-
20 structure; and

21 (C) provides the services described in sub-
22 paragraph (B) to a Federal department or
23 agency.

24 (6) DIRECTOR.—The term “Director” means
25 the Director of the National Security Agency.

1 (7) FOREIGN ADVERSARY COUNTRY.—The term
2 “foreign adversary country” has the meaning given
3 such term in section 2(c) of the Protecting Ameri-
4 cans’ Data from Foreign Adversaries Act of 2024
5 (15 U.S.C. 9901(c)).

6 (8) FOREIGN ENTITY OF CONCERN.—The term
7 “foreign entity of concern” means—

8 (A) a foreign adversary country; or

9 (B) any entity that is controlled or acting
10 under the direction of a foreign adversary coun-
11 try.

12 (9) INTELLIGENCE.—The term “intelligence”
13 has the meaning given such term in section 3 of the
14 National Security Act of 1947 (50 U.S.C. 3003).

15 (10) INTELLIGENCE COMMUNITY.—The term
16 “intelligence community” has the meaning given
17 such term in section 3 of the National Security Act
18 of 1947 (50 U.S.C. 3003).

19 (11) SECURITY CLEARANCE.—The term “secu-
20 rity clearance” means an authorization to access
21 classified information.

22 (12) THREAT INFORMATION.—The term
23 “threat information” means information on—

24 (A) efforts by foreign adversary countries
25 to use products or research of covered persons

1 or other entities or individuals to generate syn-
2 thetic media for foreign-directed influence cam-
3 paigns, develop and manage computer network
4 exploitation campaigns, design or develop weap-
5 ons systems, or enhance surveillance capabilities
6 in ways that undermine the privacy or threaten
7 the security of citizens of the United States;

8 (B) threats posed by foreign entities of
9 concern, including indications of compromise to
10 networks associated with covered persons or
11 other technical indicators, indicating a com-
12 promise to the confidentiality, integrity, or
13 availability of an artificial intelligence system,
14 or to the supply chain of an artificial intel-
15 ligence system, including training or test data,
16 frameworks or software libraries, training or in-
17 ference computing environments, or other com-
18 ponents necessary for the training, manage-
19 ment, deployment, or maintenance of an artifi-
20 cial intelligence system;

21 (C) activity of foreign entities of concern
22 to clandestinely, fraudulently, or otherwise mali-
23 ciously access the systems of covered persons
24 for purposes of illicit technology transfer or oth-
25 erwise gaining unfair economic advantage, in-

1 cluding through techniques to extract a model's
2 technical capabilities to replicate, develop, or
3 improve a foreign artificial intelligence model
4 without authorization by the covered person;

5 (D) activity of foreign entities of concern
6 to sabotage or otherwise clandestinely degrade
7 artificial intelligence systems or the supply
8 chain of an artificial intelligence system, includ-
9 ing training or test data, frameworks or soft-
10 ware libraries, training or inference computing
11 environments, or other components necessary
12 for the training, management, or maintenance
13 of an artificial intelligence system;

14 (E) observations, emerging concerns, or
15 other inputs from vendors or researchers re-
16 garding relevant malicious or clandestine activ-
17 ity of foreign entities of concern toward an arti-
18 ficial intelligence system, its supply chain, or
19 other necessary components;

20 (F) efforts by foreign adversaries or for-
21 eign entities to evade detection of malicious ac-
22 tivity described in subparagraphs (A), (B), (C)
23 and (D); and

24 (G) any other relevant information the Di-
25 rector of the National Counterintelligence and

1 Security Center and the Assistant Director of
2 the Federal Bureau of Investigation for the
3 Counterintelligence Division deem appropriate.

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

17 (1) activity of foreign entities of concern to
18 clandestinely, fraudulently, or otherwise maliciously
19 access the systems of covered persons for purposes
20 of illicit technology transfer or otherwise gaining un-
21 fair economic advantage, including through tech-
22 niques to extract a model’s technical capabilities to
23 replicate, develop, or improve a foreign artificial in-
24 telligence model without authorization by the covered
25 person;

1 (2) activity of foreign entities of concern to sab-
2 otage or otherwise clandestinely degrade artificial in-
3 telligence systems or the supply chain of an artificial
4 intelligence system, including training or test data,
5 frameworks or software libraries, training or infer-
6 ence computing environments, or other components
7 necessary for the training, management, or mainte-
8 nance of an artificial intelligence system; and

9 (3) threat information, usage trends, or other
10 input from vendors or researchers regarding ob-
11 served malicious or clandestine activity of foreign en-
12 tities of concern toward an artificial intelligence sys-
13 tem, its supply chain, or other necessary compo-
14 nents.

15 (c) ESTABLISHMENT OF PILOT PROGRAM ON SHAR-
16 ING OF INTELLIGENCE AND THREAT INFORMATION WITH
17 COVERED PERSONS.—

18 (1) IN GENERAL.—Not later than 180 days
19 after the date of the enactment of this Act, the Di-
20 rector shall, in consultation with the Director of the
21 Cybersecurity and Infrastructure Security Agency,
22 establish a pilot program to assess the feasibility
23 and advisability of facilitating the secure sharing
24 with covered persons of intelligence and threat infor-
25 mation germane to the securing of the supply chain

1 risks associated with training and maintaining artificial intelligence models procured by the Federal Government.
2
3

4 (2) PARTICIPATION.—The Director may not select or exclude covered persons to participate in the pilot program in a manner that provides a competitive advantage or procurement preference to any covered person, to the detriment of another covered person.
5
6
7
8
9

10 (3) DURATION.—The Director shall carry out the pilot program established pursuant to paragraph (1) for not less than a 3-year period beginning on the date of the establishment of the pilot program.
11
12
13

14 (d) PARTICIPATION REQUIREMENTS.—

15 (1) CRITERIA.—The Director shall establish criteria governing engagement with covered persons under the pilot program required by subsection (c), which may include criteria relating to the following:
16
17
18

19 (A) Relevance to national security.

20 (B) The ability to protect classified or sensitive intelligence information.
21

22 (C) Cybersecurity and information security maturity.
23

24 (D) Agreement to comply with intelligence handling, use, and nondisclosure requirements.
25

1 (E) The availability of cleared personnel of
2 covered persons or willingness of covered per-
3 sons to increase the number of cleared per-
4 sonnel.

5 (2) NATURE OF PARTICIPATION.—Participation
6 in the pilot program required by subsection (c) shall
7 not be construed as a certification, endorsement, or
8 regulatory approval by the United States Govern-
9 ment of any artificial intelligence system or commer-
10 cial activity and the Director may not exclude a cov-
11 ered person from participating on the basis of polit-
12 ical or ideological viewpoints of the covered person
13 or its employees.

14 (e) INTELLIGENCE SHARING STRUCTURE.—

15 (1) AUTHORIZED MODES.—Under the pilot pro-
16 gram required by subsection (c), the Director may
17 authorize the sharing of intelligence and threat in-
18 formation as described in paragraph (1) of such sub-
19 section through—

20 (A) bilateral exchanges between elements
21 of the intelligence community and a covered
22 person;

23 (B) multilateral exchanges among covered
24 persons, as determined appropriate by the Di-
25 rector; or

1 (C) another designated intelligence-sharing
2 mechanism operated or overseen by the Direc-
3 tor.

4 (2) LIMITATION.—Any mechanism established
5 under this section shall be limited to the dissemina-
6 tion of intelligence and threat information and shall
7 not establish standards, requirements, or best prac-
8 tices governing artificial intelligence development or
9 deployment.

10 (f) TAILORING, HANDLING, AND PROTECTION OF IN-
11 TELLIGENCE.—

12 (1) PROCEDURES REQUIRED.—The Director
13 shall codify procedures to tailor, sanitize, or down-
14 grade the classification level of intelligence shared
15 under the pilot program required by subsection (c)
16 to ensure usability while protecting intelligence
17 sources and methods.

18 (2) EXAMPLES OF PROCEDURES.—The proce-
19 dures developed under paragraph (1) may include
20 the following:

21 (A) The use of tear lines and segregable
22 summaries.

23 (B) The preparation of classified annexes
24 where necessary.

1 (C) Criteria governing the classification
2 level of shared intelligence.

3 (D) The appropriate use of cleared indus-
4 try personnel.

5 (3) HANDLING REQUIREMENTS.—The Director
6 shall, acting through the Center, codify policies gov-
7 erning the handling, storage, and dissemination of
8 intelligence shared under the pilot program required
9 by subsection (c), including audit and compliance
10 mechanisms.

11 (g) PERMISSIBLE USE AND NONDISCLOSURE.—

12 (1) PERMISSIBLE USE.—Intelligence shared
13 under the pilot program required by subsection (c)
14 may be used solely for detecting, preventing, or miti-
15 gating malicious foreign activity targeting the supply
16 chains associated with training and maintaining arti-
17 ficial intelligence models procured by the Federal
18 Government for intelligence collection, intellectual
19 property theft, and other malicious activities.

20 (2) NONDISCLOSURE.—A covered person par-
21 ticipating in the pilot program may not disclose any
22 intelligence shared under the pilot program required
23 by subsection (c), except as expressly authorized by
24 the Director acting through the Center.

1 (h) PRIVACY AND CIVIL LIBERTIES.—In planning
2 and coordinating the pilot program required by subsection
3 (c), the Director shall, acting through the Center, consult
4 with the Civil Liberties Protection Officer of the Office
5 of the Director of National Intelligence.

6 (i) EVALUATION AND REPORTING.—

7 (1) EVALUATION.—The Director shall continu-
8 ously evaluate the effectiveness and risks of the pilot
9 program established under subsection (c).

10 (2) REPORT.—

11 (A) IN GENERAL.—Not later than 90 days
12 before the date on which the pilot program re-
13 quired by paragraph (1) of subsection (c) termi-
14 nates pursuant to paragraph (3) of such sub-
15 section, the Directors shall submit to the con-
16 gressional intelligence committees (as defined in
17 section 3 of the National Security Act of 1947
18 (50 U.S.C. 30003)) a report assessing—

19 (i) the effectiveness of intelligence
20 sharing under the pilot program;

21 (ii) the adequacy of safeguards for
22 sources, methods, and privacy;

23 (iii) the scope of participation and list
24 of covered persons participating in the
25 pilot program; and

1 (iv) whether the program should be
2 modified, extended, or terminated.

3 (B) FORM.—The report submitted pursu-
4 ant to subparagraph (A) shall be submitted in
5 unclassified form, but may include a classified
6 annex.

7 (j) RULE OF CONSTRUCTION.—Nothing in this sec-
8 tion shall be construed—

9 (1) to authorize the collection of intelligence on
10 United States persons not authorized by another
11 provision of law;

12 (2) to require the disclosure of classified infor-
13 mation to unauthorized persons; or

14 (3) to establish commercial, competition, or
15 technology policy outside the purview of the intel-
16 ligence community.

17 (k) EXEMPTION FROM DISCLOSURE; PROTECTION.—
18 Any information shared by a covered person or other enti-
19 ty or individual with the United States Government pursu-
20 ant to this section—

21 (1) shall be exempt from disclosure and with-
22 held, without discretion, from the public, pursuant
23 to section 552(b)(3)(B) of title 5, United States
24 Code, and any other provision of United States law
25 or law of any State, political subdivision or agency

1 thereof, or Tribe requiring disclosure of information
2 or records; and

3 (2) shall not be deemed a waiver of any applica-
4 ble privilege or protection, including trade secret
5 protection.

6 (1) PROTECTION FROM LIABILITY.—No cause of ac-
7 tion shall lie or be maintained in any court against any
8 covered person for sharing information with the United
9 States Government or another covered person pursuant to
10 this section.