.....

(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to establish within the Cybersecurity and Infrastructure Security Agency the National Cyber and AI Investigations Board to investigate significant cyber incidents, cyber incidents involving terrorism, and cyber incidents involving artificial intelligence, to determine root causes and develop recommendations to prevent similar incidents and address terrorism threats to the United States, including threats relating to the malicious use of information systems or artificial intelligence by covered foreign adversaries, including terrorist organizations, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To amend the Homeland Security Act of 2002 to establish within the Cybersecurity and Infrastructure Security Agency the National Cyber and AI Investigations Board to investigate significant cyber incidents, cyber incidents involving terrorism, and cyber incidents involving artificial intelligence, to determine root causes and develop recommendations to prevent similar incidents and address terrorism threats to the United States, including threats relating to the malicious use of information sys-

tems or artificial intelligence by covered foreign adversaries, including terrorist organizations, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Reviewing Origins, Outcomes, and Threats from Cyber and Artificial Intelligence to Understand Security Events Act'' or the ''ROOT CAUSE Act''.

SEC. 2. NATIONAL CYBER AND AI INVESTIGATIONS NCAI BOARD.

Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 650 et seq.) is amended by adding at the end the following new subtitle:

''Subtitle E—National Cyber and AI Investigations Board

''SEC. 2251. ESTABLISHMENT, MISSION, AND ORGANIZATION.

''(a) ESTABLISHMENT.—There is established within the Agency a board to be known as the 'National Cyber and AI Investigations NCAI Board' (in this subtitle referred to as the 'NCAI Board').

''(b) MISSION.—The mission of the NCAI Board is to conduct independent, impartial, and technically rig-

orous reviews of covered incidents in order to carry out the following:

''(1) Determine the facts, circumstances, root causes, and contributing factors of each covered incident that is reviewed.

''(2) Evaluate the effectiveness of the preventive measures, detection capabilities, mitigation activities, and response actions of affected entities, responding entities, and executive agencies, including the Department and the Agency, taking into account each such entity's role, operational control, and information reasonably available at the time of such a covered incident.

''(3) Identify threat activity and the tactics, techniques, and procedures of threat actors, including covered foreign adversaries, terrorist organizations, criminal organizations, and individuals acting alone, and the use by such threat actors of artificial intelligence systems.

''(4) Develop specific, actionable, and prioritized recommendations to prevent, detect, mitigate, and respond to similar incidents, taking into account technical feasibility and the responsibilities and capabilities of the entities to which such recommendations are directed.

''(5) Disseminate lessons learned to owners and operators of critical infrastructure, SLTT entities, the private sector, the Homeland Security Enterprise, the public, and the Federal Government to strengthen the security and resilience of the homeland against cybersecurity risks, including such risks caused by an act of terrorism.

''(6) Assess terrorism threats to the United States demonstrated by a covered incident under review, including threats relating to the malicious use of information systems or artificial intelligence systems by covered foreign adversaries, including terrorist organizations, and develop recommendations to address such threats.

''(c) SCOPE.—The NCAI Board may review a covered incident affecting or involving any of the following:

''(1) A non-Federal information system, including an information system or operational technology that supports critical infrastructure.

''(2) An information system owned or operated by or on behalf of an executive agency, other than a national security system.

''(3) An artificial intelligence system or any component, resource, or environment used to develop, train, test, evaluate, deploy, operate, secure,

or provide access to such a system, including an artificial intelligence model, model weights, training or evaluation data, training or evaluation infrastructure, agent tools, interfaces, and safeguards, including such systems, components, resources, or environments owned by Federal contractors that are used for Federal Government purposes or connected to executive agency information systems.

''(4) A software or hardware product, digital or cloud service, managed service, communications network, or technology supply chain that caused or materially contributed to a covered incident affecting, or the effects of a covered incident on, a system described in paragraph (1), (2), or (3), including a vulnerability, compromise, defect, or failure affecting, or capable of affecting, multiple persons or entities.

''(d) NATURE OF REVIEWS.—

''(1) FACTUAL INQUIRY.—Each review under this section shall be a factual inquiry directed at preventing future covered incidents. In carrying out such a review, the NCAI Board may make findings regarding any act, omission, practice, or decision of any person or entity that caused or contributed to a covered incident.

''(2) NO DETERMINATION OF LIABILITY.—In carrying out a review under this section, or in making any finding or issuing any report relating to such a review, the NCAI Board may not—

''(A) determine the rights or liabilities of any person; or

''(B) assign civil or criminal culpability.

''(3) NONREGULATORY BODY.—The NCAI Board shall have no regulatory, enforcement, or sanction authority, and no recommendation of the NCAI Board shall have the force or effect of law.

''(e) ORGANIZATION AND SUPPORT.—

''(1) ADMINISTRATIVE SUPPORT.—The Director shall provide the NCAI Board with the administrative, logistical, security, facilities, information technology, legal, and budgetary support necessary to carry out this subtitle.

''(2) INDEPENDENT JUDGMENT.—Subject to section 2261, the NCAI Board shall exercise independent judgment in selecting covered incidents for review, determining the scope and conduct of such reviews, and adopting findings and recommendations relating thereto.

''(3) REVIEWS INVOLVING THE DEPARTMENT.—If the actions of the Agency or any other component

of the Department are relevant to a covered incident under review, the NCAI Board shall evaluate such actions with the same rigor applied to an evaluation of any other entity, and no officer or employee of the Agency or such other component who was personally and substantially involved in such actions may participate in such review on behalf of the NCAI Board.

''(4) SEPARATE BUDGET DISPLAY.—The Secretary shall include in the budget justification materials submitted to Congress in support of the budget of the Department for each fiscal year a separate display of the amounts and full-time equivalent positions requested for the NCAI Board.

''(f) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE ACT.—Chapter 10 of title 5, United States Code (commonly known as the 'Federal Advisory Committee Act'), shall not apply to the NCAI Board or to any subcommittee of the NCAI Board.

''SEC. 2252. MEMBERSHIP.

''(a) COMPOSITION.—The NCAI Board shall be composed of nine voting members appointed by the Secretary, as follows:

''(1) Three full-time members, including the Chair, each of whom shall be an officer or employee

of the Department appointed to serve on the NCAI Board on a full-time basis.

''(2) Six part-time members, each of whom shall be an individual who is not otherwise an officer or employee of the Federal Government and who shall serve as a special Government employee (as such term is defined in section 202(a) of title 18, United States Code).

''(b) QUALIFICATIONS.—

''(1) IN GENERAL.—Each member of the NCAI Board shall be appointed solely on the basis of integrity and demonstrated expertise and experience in cybersecurity, incident response, digital forensics, artificial intelligence, critical infrastructure operations, national security, or another field relevant to the mission of the NCAI Board, and shall have not less than seven years of professional experience in one or more of such fields.

''(2) FULL-TIME MEMBERS.—Of the full-time members, at least one shall have demonstrated experience leading complex technical investigations or incident response engagements, and at least one shall have demonstrated expertise in the security of artificial intelligence systems, including artificial intelligence agents.

''(3) PART-TIME MEMBERS.—The part-time members of the NCAI Board shall collectively possess demonstrated expertise in each of the following areas:

''(A) The security of information technology systems.

''(B) The security of operational technology and industrial control systems.

''(C) The security, development, testing, evaluation, and deployment of advanced artificial intelligence systems, including artificial intelligence agents.

''(D) Cloud computing, identity and access management, and software supply chain security.

''(E) Incident response, threat intelligence, and digital forensics.

''(F) The operation of critical infrastructure, including by small and rural owners and operators.

''(G) The cybersecurity of SLTT entities.

''(H) National security threats posed by covered foreign adversaries and terrorist organizations, including threats involving chemical, biological, radiological, or nuclear weapons.

''(4) BALANCE.—Not more than three part-time members of the NCAI Board may, at any time, be officers, employees, or paid consultants of an entity that develops, sells, or provides cybersecurity, cloud computing, software, telecommunications, or artificial intelligence products or services. In appointing part-time members, the Secretary shall give consideration to individuals who previously held senior technical, operational, or security leadership positions in industry, academia, or government.

''(5) ELIGIBILITY.—Each member of the NCAI Board shall be a citizen of the United States, and shall be eligible to obtain and maintain a security clearance at the top secret level with access to sensitive compartmented information. No individual may serve as such a member if such individual satisfies any of the following criteria:

''(A) Is registered, or is required to register, as an agent of a foreign principal under the Foreign Agents Registration Act of 1938 (22 U.S.C. 611 et seq.).

''(B) Received compensation, during the 5-year period preceding appointment to the NCAI Board, from a covered foreign adversary or an entity domiciled in a covered foreign country.

''(C) During the 2-year period preceding appointment to the NCAI Board, served as a noncareer appointee in a the Senior Executive Service position (as such terms are defined in section 3132(a) of title 5, United States Code), served in a position of a confidential or policy determining character under schedule C of subpart C of part 213 of title 5, Code of Federal Regulations, or served as an officer or employee of a national, State, or local committee of a political party or of an authorized campaign committee of a candidate for Federal, State, or local office.

''(6) POLITICAL BALANCE.—

''(A) IN GENERAL.—Not more than five members of the NCAI Board may be appointed from the same political party, and not more than two full-time members of the NCAI Board may be appointed from the same political party.

''(B) ALTERNATE MEMBERS.—The Chair may not designate an alternate member under subsection (d)(2) with respect to a review under section 2251 if the result of such designation would be that more than five of the individuals

voting with respect to such review would have been appointed from the same political party.

''(7) FULL-TIME MEMBERS SERVE IN CAREER POSITIONS.—During service on the NCAI Board, a full-time member may not serve as a noncareer appointee in a Senior Executive Service position or in a position of a confidential or policy determining character under schedule C of subpart C of part 213 of title 5, Code of Federal Regulations.

''(c) NONVOTING PARTICIPANTS.—

''(1) AGENCY LIAISON.—The Director may designate an officer or employee of the Agency to serve as a nonvoting liaison to the NCAI Board, except that such liaison may not participate in any deliberation of the NCAI Board relating to findings or recommendations regarding the actions of the Agency.

''(2) OTHER EXECUTIVE AGENCY LIAISONS.—The Chair may invite the head of any executive agency, including any Sector Risk Management Agency and any executive agency with authority to investigate accidents or incidents affecting critical infrastructure, to designate an officer or employee of such executive agency to serve as a nonvoting liaison to the NCAI Board, either generally or with respect

to a particular review under section 2251. A liaison designated under this paragraph may not participate in any deliberation of the NCAI Board relating to findings or recommendations regarding the actions of the executive agency of such liaison.

''(3) TECHNICAL ADVISORS.—The Chair may appoint, for the duration of a particular review under section 2251, individuals with specialized expertise to serve as nonvoting technical advisors to the NCAI Board. Any such technical advisor who is not otherwise an officer or employee of the Federal Government shall serve as a special Government employee.

''(d) ALTERNATE MEMBERS.—

''(1) APPOINTMENT.—The Secretary may appoint not more than four alternate members of the NCAI Board, each of whom shall satisfy the qualifications and eligibility requirements applicable to part-time members.

''(2) SERVICE.—The Chair may designate an alternate member to serve in place of a part-time member who is recused in accordance with section 2254 from a review under section 2251. An alternate member so designated shall have the rights and

duties of a part-time member solely with respect to such review.

''(e) TERMS.—

''(1) FULL-TIME MEMBERS.—Each full-time member of the NCAI Board shall be appointed for a term of five years.

''(2) PART-TIME AND ALTERNATE MEMBERS.—Each part-time member and alternate member of the NCAI Board shall be appointed for a term of three years, except that, of the part-time members first appointed, two shall be appointed for a term of one year, two shall be appointed for a term of two years, and two shall be appointed for a term of three years, as designated by the Secretary at the time of appointment.

''(3) LIMITATION.—No individual may serve more than two consecutive full terms as a member of the NCAI Board.

''(4) CONTINUATION OF SERVICE.—A member of the NCAI Board may continue to serve after the expiration of the term of such member until a successor is appointed, except that such member may not continue to serve for more than one year after such expiration.

''(5) VACANCIES.—A vacancy on the NCAI Board shall not affect the powers of the NCAI Board and shall be filled, not later than 90 days after the date on which such vacancy occurs, in the same manner as the original appointment. An individual appointed to fill a vacancy shall serve for the remainder of the term of the member being replaced.

''(f) REMOVAL.—

''(1) IN GENERAL.—The Secretary may remove a member or alternate member of the NCAI Board.

''(2) NOTIFICATION.—Not later than 15 days after removing a member or alternate member of the NCAI Board under this subsection, the Secretary shall notify the appropriate congressional committees in writing of such removal and the reasons relating thereto, including whether such removal related to any ongoing review under section 2251 or to any finding, recommendation, or report of the NCAI Board.

''(3) STATEMENT OF REMOVED MEMBER.—A member removed under paragraph (1) may, not later than 30 days after such removal, submit to the appropriate congressional committees a written statement regarding such removal.

''(4) MULTIPLE REMOVALS.—If two or more members are removed during any 12-month period, the Secretary shall, not later than 14 days after the second and each subsequent such removal, brief the appropriate congressional committees on the reasons for such removals, the effect of such removals on any ongoing review under section 2251, and the timeline for filling each resulting vacancy in accordance with this section.

''(g) COMPENSATION AND EXPENSES.—A part-time member, alternate member, or technical advisor of the NCAI Board who is not otherwise an officer or employee of the Federal Government may not receive pay by reason of service on the NCAI Board, but shall be allowed travel expenses, including per diem in lieu of subsistence, in accordance with section 5703 of title 5, United States Code.

''(h) REQUIREMENTS.—Each member, alternate member, and technical advisor of the NCAI Board shall carry out the following:

''(1) Complete all financial disclosure reports and ethics training required by law.

''(2) Obtain and maintain a security clearance appropriate to the duties of such member, alternate member, or technical advisor, as the case may be.

''(3) Sign and adhere to nondisclosure agreements pertaining to the work of the NCAI Board.

''(4) Serve in a personal capacity and not as a representative of any current or former employer or client.

''(i) QUORUM AND VOTING.—A majority of the voting members of the NCAI Board who are not recused in accordance with section 2254, including at least one full-time member, shall constitute a quorum. Except as otherwise provided in this subtitle, the NCAI Board shall act by a majority vote of the voting members present and not so recused. An alternate member designated under subsection (d)(2) shall be counted as a voting member with respect to the review under section 2251 for which such alternate member is designated.

''(j) MEETINGS.—The NCAI Board shall meet at the call of the Chair, and not less frequently than quarterly. Meetings of the NCAI Board may be closed to the public.

"SEC. 2253. CHAIR, EXECUTIVE DIRECTOR, AND STAFF.

''(a) CHAIR AND VICE CHAIR.—

''(1) DESIGNATION.—The Secretary shall designate the Chair of the NCAI Board from among the full-time members of the NCAI Board and the Vice Chair of the NCAI Board from among the part-time members of the NCAI Board.

''(2) DUTIES OF THE CHAIR.—The Chair shall manage the affairs of the NCAI Board, including by carrying out the following:

''(A) Convening and presiding over meetings of the NCAI Board.

''(B) Developing, with the approval of the NCAI Board, bylaws and procedures for the conduct of reviews under section 2251, including procedures governing technical assistance under subsection (d) of section 2256 and factual accuracy review under subsection (j) of such section, and publishing such bylaws and procedures on the website required under section 2260(e).

''(C) Entering into contracts, interagency agreements, and memoranda of understanding necessary to carry out this subtitle.

''(D) Serving as the principal point of contact of the NCAI Board with the appropriate congressional committees.

''(3) VICE CHAIR.—The Vice Chair shall carry out the duties of the Chair in the absence of the Chair, except that the Vice Chair may not exercise any authority reserved to full-time members under section 2257.

''(b) EXECUTIVE DIRECTOR.—The Secretary, on the recommendation of the Chair, shall appoint an Executive Director of the NCAI Board, who shall be a career appointee (as such term is defined in section 3132(a) of title 5, United States Code) and who shall, under the direction of the Chair, manage the staff and daily operations of the NCAI Board.

''(c) STAFF.—

''(1) IN GENERAL.—The Secretary shall provide the NCAI Board with permanent full-time staff sufficient to carry out this subtitle, including investigators, digital forensic analysts, threat intelligence analysts, artificial intelligence researchers and model evaluators, software, cloud, and operational technology engineers, attorneys, privacy specialists, and technical writers.

''(2) STAFFING LEVEL.—The Secretary shall ensure the number of full-time equivalent positions dedicated to supporting the NCAI Board is sufficient to carry out this subtitle. The Chair shall include in each annual report under section 2260(f) an assessment of the staffing and resources necessary to carry out this subtitle and of any shortfall in such staffing and resources.

''(3) HIRING AUTHORITY.—The Secretary may exercise the authority provided under section 2208 with respect to positions on the staff of the NCAI Board.

''(4) DETAILEES.—The head of any executive agency may detail personnel to the NCAI Board on a reimbursable or nonreimbursable basis.

''(5) CONTRACTING.—The NCAI Board may contract for specialized technical services, including forensic analysis, malware analysis, artificial intelligence evaluation, and reproduction and validation of attack paths and adversary emulation, subject to the following:

''(A) All findings, conclusions, and recommendations, and each report of the NCAI Board, shall be the work of the NCAI Board.

''(B) The NCAI Board may not enter into a contract with any person who has a conflict of interest, as determined under the policy established under section 2254(a), with respect to the review under section 2251 for which such services are procured.

''(C) Any contractor providing specialized technical services under this paragraph shall be subject to a statutory nondisclosure agreement

prohibiting the retention, disclosure, reverse engineering, or commercial use of any proprietary artificial intelligence model—

"(i) prompt,

"(ii) output,

"(iii) system log, or

"(iv) telemetry,

accessed in connection with such services.

"(d) TECHNICAL CAPABILITIES.—

"(1) IN GENERAL.—The Secretary shall ensure the NCAI Board has access to the forensic and analytic tools, secure computing environments, and facilities for the storage and discussion of classified information necessary to carry out this subtitle.

"(2) ARTIFICIAL INTELLIGENCE TOOLS.—The NCAI Board may use artificial intelligence systems to support the analysis of information obtained in the course of a review under section 2251, including logs, transcripts of artificial intelligence agent activity, and other large data sets, subject to the following:

"(A) The NCAI Board shall maintain access to artificial intelligence systems developed by more than one developer.

''(B) To the extent practicable, the NCAI Board may not use an artificial intelligence system developed, owned, or operated by an entity the conduct of which is the subject of a review under section 2251 to analyze information relating to such entity.

''(C) The NCAI Board shall ensure the following:

''(i) Any artificial intelligence system used under this paragraph is deployed in a manner that prevents the provider of such system from retaining information obtained by the NCAI Board or using such information to train any artificial intelligence model.

''(ii) Any such analysis is performed in an isolated, air-gapped, or zero-data-retention environment.

''(D) The NCAI Board may not procure, obtain, or use any artificial intelligence system or model developed, produced, owned, or controlled by a covered foreign adversary or by an entity domiciled in a covered foreign country, except that the NCAI Board may use such a system or model in a secure and isolated envi-

ronment to the extent necessary to evaluate such a system or model in the course of a review under section 2251.

"SEC. 2254. ETHICS, CONFLICTS OF INTEREST, AND RECUSAL.

"(a) POLICY.—Not later than 180 days after the date of the enactment of this subtitle, the Secretary, in consultation with the Chair and the designated agency ethics official of the Department, shall publish on the website required under section 2260(e) a proposed policy to identify, disclose, mitigate, and manage conflicts of interest of members, alternate members, technical advisors, staff, and contractors of the NCAI Board, solicit for a period of not fewer than 30 days public comment on such proposed policy, and, not later than 90 days after the close of such comment period, publish the final policy relating thereto. Such policy shall include the following:

"(1) Criteria and procedures for the mandatory recusals required under subsection (b), including thresholds for disqualifying financial interests and criteria for determining whether an entity described in subsection (b)(2) is a direct competitor of an entity the conduct of which is the subject of a review under section 2251.

''(2) Procedures for the disclosure of financial interests and of employment, consulting, and client relationships relevant to each review under section 2251.

''(3) Procedures governing recusal at each stage of a review under section 2251, including the selection of a covered incident for such a review, decisions regarding preservation notices and subpoenas under section 2257, the conduct of such a review, the adoption of findings and recommendations, and the approval of reports.

''(4) Procedures for the designation of alternate members under section 2252(d).

''(b) MANDATORY RECUSAL.—A member, alternate member, technical advisor, or staff member of the NCAI Board shall be recused from all participation in a review under section 2251 if any of the following applies:

''(1) Such individual is, or during the 2-year period preceding the initiation of such review was, an officer, director, employee, contractor, or paid consultant of, or an attorney or other professional advisor to—

''(A) an entity the conduct of which is the subject of such review; or

''(B) an entity materially affected by the covered incident under such review.

''(2) An entity with respect to which such individual is, or during such 2-year period was, an officer, director, employee, contractor, or paid consultant, or to with respect to which such individual is, or during such period was, an attorney or other professional advisor, is a direct competitor, as determined under the policy established under subsection (a), of an entity the conduct of which is the subject of such review.

''(3) Such individual has a financial interest in an entity described in paragraph (1) or (2) that exceeds the threshold established under the policy established under subsection (a).

''(4) Such individual was personally and substantially involved in the response to the covered incident under review under section 2251, including as an officer or employee of an executive agency the actions of which are the subject of such review.

''(c) LIMITED PARTICIPATION.—An individual recused under subsection (b) may, at the request of the NCAI Board, provide factual or technical information to the NCAI Board relating to the review at issue under sec-

tion 2251, but may not participate in any deliberation or vote relating to such review.

''(d) PUBLIC DISCLOSURE OF RECUSALS.—The NCAI Board shall disclose the name of each member and alternate member recused from a review under section 2251, and the general basis for each such recusal, in the public notice of initiation of such review under section 2255(g) and in the final report relating to such review, except to the extent such disclosure would reveal classified information.

''(e) RESTRICTIONS ON FULL-TIME MEMBERS AND STAFF.—

''(1) FINANCIAL INTERESTS.—No full-time member or staff member of the NCAI Board may hold a financial interest in an entity the conduct of which is the subject of an ongoing review under section 2251 in which such individual participates. The Secretary may issue supplemental standards of ethical conduct for full-time members and staff of the NCAI Board, consistent with applicable law.

''(2) COMMITMENT AFTER SERVICE.—

''(A) IN GENERAL.—As a condition of appointment to the NCAI Board, each member of the NCAI Board and each staff member of the NCAI Board serving in an investigative position

shall agree in writing that, during the 2-year period after conclusion of the service of such individual with the NCAI Board, such individual will not knowingly make, with the intent to influence, any communication to or appearance before the NCAI Board on behalf of any person other than the United States in connection with any review under section 2251. The NCAI Board may not accept any such communication or appearance, and the Chair shall report to the appropriate congressional committees any violation of such an agreement.

''(B) FURTHER REQUIREMENTS.—In addition to the condition described in subparagraph (A), each member of the NCAI Board and staff member of the NCAI Board serving in an investigative position shall agree in writing that, during the 1-year period after the conclusion of the service of such individual with the NCAI Board, such individual will not accept employment, compensation, or equity from any direct commercial competitor of an entity the proprietary artificial intelligence models, source code, or internal security architecture of which were

reviewed or evaluated by individual during such period of service.

''(f) CONTRACTORS AND TECHNICAL ASSISTANCE.—The requirements of subsection (b) shall apply, as appropriate, to any contractor supporting the NCAI Board with respect to a review under section 2251. The Chair shall ensure no person providing technical assistance under section 2256(d) is given access to the proprietary information of any other person.

''SEC. 2255. SELECTION OF COVERED INCIDENTS FOR REVIEW.

''(a) AUTHORITY.—The NCAI Board may, by majority vote, initiate a review under section 2251 of any covered incident, including a covered incident that occurred before the date of the enactment of this subtitle.

''(b) REFERRALS.—Any of the following may refer a cyber incident to the NCAI Board for consideration for a review under section 2251:

''(1) The President.

''(2) The Secretary.

''(3) The Director.

''(4) The head of any Sector Risk Management Agency.

''(5) The chair or ranking member of an appropriate congressional committee.

''(6) Any member of the NCAI Board.

''(c) PUBLIC RECOMMENDATIONS.—The NCAI Board shall establish a mechanism through which any person may recommend a cyber incident to the NCAI Board for consideration for a review under section 2251.

''(d) MANDATORY CONSIDERATION.—

''(1) TRIGGERING EVENTS.—The NCAI Board shall vote on whether to initiate a review under section 2251 of a cyber incident not later than 30 days after the occurrence of any of the following:

''(A) The Secretary declares a significant incident under section 2233 with respect to such cyber incident.

''(B) The Federal Government establishes a unified coordination group, or an equivalent interagency coordination mechanism, to coordinate the response to such cyber incident.

''(C) The Secretary determines, or the NCAI Board has reason to believe, that such cyber incident is a cyber incident involving terrorism or is a covered chemical, biological, radiological, or nuclear incident.

''(D) The NCAI Board receives a referral of such cyber incident under subsection (b) from the President, the Secretary, or the chair

or ranking member of an appropriate congressional committee.

''(2) NOTIFICATION TO THE NCAI BOARD.—The Secretary shall notify the Chair not later than 48 hours after the occurrence of an event described in subparagraph (A) or (B) of paragraph (1), or after making a determination described in subparagraph (C) of such paragraph.

''(3) NOTICE OF DECISION.—Not later than seven days after a vote under paragraph (1), the NCAI Board shall notify the appropriate congressional committees, and any official who referred to the NCAI Board the cyber incident at issue, of the decision of the NCAI Board and the reasons relating thereto, with reference to the criteria established under subsection (f).

''(e) PRESUMPTION OF REVIEW.—With respect to a cyber incident described in subparagraph (A) or (C) of subsection (d)(1), the NCAI Board shall initiate a review under section 2251 unless a majority of the voting members determines in writing that any of the following applies:

''(1) Such a review is not warranted under the criteria established under subsection (f).

''(2) Such a review would substantially duplicate another review under such section, investigation, or report that adequately addresses the matters described in section 2256(a).

''(3) The NCAI Board lacks the resources to conduct such a review without compromising an ongoing review under section 2251 of higher priority, in which case the NCAI Board shall include in the notice required under subsection (d)(3) the date on which the NCAI Board will reconsider such determination.

''(f) SELECTION CRITERIA.—

''(1) IN GENERAL.—Not later than 180 days after the date of the first meeting of the NCAI Board, the NCAI Board shall publish on the website required under section 2260(e) proposed criteria for the selection of covered incidents for review under section 2251, solicit for a period of not fewer than 30 days public comment on such proposed criteria, and, not later than 90 days after the close of such comment period, publish final criteria for such selection.

''(2) FACTORS.—Final criteria published pursuant to paragraph (1) shall address the following fac-

tors with respect to the selection of a covered incident for review under section 2251:

''(A) The severity and scale of actual or potential harm to national security, economic security, public health and safety, public confidence, or civil liberties reasonably likely to result from such a covered incident.

''(B) The extent to which the causes of such covered incident could affect other information systems, entities, or sectors, including through common technologies, platforms, service providers, suppliers, or artificial intelligence systems.

''(C) The novelty of the tactics, techniques, or procedures involved, including any novel use of artificial intelligence systems or artificial intelligence agents and any previously unobserved capability, and whether such novelty is reasonably likely to result in actual or potential harm to national security, economic security, public health or safety, public confidence, or civil liberties, except that harm to public confidence, on its own, shall not establish a covered incident as eligible for such selection.

''(D) The involvement of a covered foreign adversary or a terrorist organization, or whether such covered incident is a cyber incident involving terrorism.

''(E) Any nexus to chemical, biological, radiological, or nuclear weapons.

''(F) The potential of such review to identify gaps in policy, practice, standards, law, or the capabilities of executive agencies.

''(G) The effects of such covered incident on SLTT entities, small businesses, and rural communities.

''(H) The extent to which lessons from such covered incident are already available through other reviews or reports.

''(I) The relationship of such covered incident to prior reviews under such section, and to patterns across multiple cyber incidents.

''(J) The feasibility of obtaining the information necessary to conduct such review and the resources available to the NCAI Board.

''(3) UPDATES.—The NCAI Board shall review and, as appropriate, update the final criteria published pursuant to paragraph (1) not less frequently

than once every two years, in accordance with the procedures described in such paragraph.

''(g) NOTICE OF INITIATION.—

''(1) CONGRESSIONAL NOTICE.—Not later than seven days after initiating a review under section 2251, the NCAI Board shall notify the appropriate congressional committees of such initiation, including a description of the covered incident that is the subject of such review, the scope of such review, the basis for the decision to initiate such review, and any recusals.

''(2) PUBLIC NOTICE.—Not later than 14 days after initiating a review under section 2251, the NCAI Board shall publish on the website required under section 2260(e) a notice that includes a general description of the covered incident that is the subject of such review, the scope of such review, the anticipated timeline for such review, and the recusals disclosed under section 2254(d). The NCAI Board shall withhold from such notice the identity of any affected person or entity the involvement of which in such covered incident has not been publicly disclosed, unless such person or entity consents to disclosure of such identification.

''(3) DELAYED PUBLIC NOTICE.—The NCAI Board may delay publication of a notice under paragraph (2) if the NCAI Board determines such publication would jeopardize an ongoing incident response, law enforcement investigation, intelligence activity, or the national security of the United States. The NCAI Board shall notify the appropriate congressional committees of any such delay and the reasons relating thereto, and shall publish on the website required under section 2260(e) such notice once such circumstances no longer apply.

''(h) SCOPE OF REVIEWS.—

''(1) DETERMINATION BY THE NCAI BOARD.—The NCAI Board shall determine the scope of each review under section 2251 and may modify such scope, including to encompass a cyber incident related to the cyber incident that is the subject of such review. The NCAI Board shall notify the appropriate congressional committees of any such modification.

''(2) NO CONDITIONAL LIMITATIONS.—The NCAI Board may not agree to any limitation on the scope, duration, or subject matter of a review under section 2251, or on access to information relevant to such a review, as a condition of the voluntary co-

operation of any person with respect to such a review.

''(i) COORDINATION WITH INCIDENT RESPONSE.—The NCAI Board shall coordinate with the Director and other responding executive agencies to avoid interfering with active incident response activities, and may defer requests for information from, or interviews of, personnel actively engaged in such activities. Nothing in this subsection limits the authority of the NCAI Board to issue a preservation notice under section 2257(b).

''(j) NATIONAL SECURITY SYSTEMS.—The NCAI Board may not review any matter relating to a national security system, or to any information system of the Department of Defense or of an element of the intelligence community, without the consent of the head of the executive agency that owns or operates such system. Nothing in this subsection prevents the NCAI Board from reviewing matters relating to any other information system affected by the same covered incident as affects the national security system, or information system of the Department of Defense or of an element of the intelligence community, at issue.

''(k) RECORD OF DECLINED INCIDENTS.—The NCAI Board shall maintain, and publish on the website required under section 2260(e), a list of each cyber incident with

respect to which the NCAI Board voted under subsection (d), or that the NCAI Board otherwise formally considered, and declined to review, together with a summary of the reasons for each such declination, except to the extent such publication would reveal classified information or information protected under section 2258.

"SEC. 2256. CONDUCT OF REVIEWS.

''(a) REQUIRED ELEMENTS.—Each review under section 2251 of a covered incident shall, to the extent practicable and relevant, examine the following:

''(1) The timeline and sequence of events of such covered incident.

''(2) The initial access vectors, security vulnerabilities, misconfigurations, and tactics, techniques, and procedures involved.

''(3) The technical, organizational, procedural, and policy root causes and contributing factors, including governance practices of affected entities and of relevant technology providers, assessed against relevant consensus standards, industry best practices, and commitments.

''(4) Whether reasonable security controls, standards, and practices, consistent with relevant consensus standards and industry best practices,

were implemented and whether such controls, standards, and practices were effective.

''(5) The detection, notification, containment, remediation, and recovery actions of affected entities, including the timeliness of detection and of notification to affected third parties and the Federal Government.

''(6) The actions of executive agencies, including the Department and the Agency, to prevent, detect, share information regarding, and respond to such covered incident, including information shared under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.) and reports submitted under subtitle D.

''(7) The effects of such covered incident, including on critical infrastructure, SLTT entities, public health and safety, and individuals.

''(8) To the extent consistent with the protection of intelligence sources and methods, and in coordination with appropriate executive agencies, the attribution of such covered incident, except that the NCAI Board may not publicly attribute such covered incident to the government of a covered foreign country or to any other covered foreign adversary

unless the Federal Government has first publicly made such attribution.

''(9) Whether such covered incident is, or is related to, a cyber incident involving terrorism, or to a campaign by a covered foreign adversary to gain or maintain access to critical infrastructure for the purpose of future disruption or destruction, except that the NCAI Board may not publicly characterize a covered incident as a cyber incident involving terrorism during the pendency of a criminal investigation or prosecution relating to such covered incident is unless the Federal Government has first publicly made such characterization.

''(10) Dependencies on outside service providers, suppliers, and software, including open source software, that contributed to such covered incident or its effects.

''(11) With respect to a covered incident that involves a ransomware attack—

''(A) the effects on public health or safety, or on the continuity of critical infrastructure services, of such ransomware attack;

''(B) any ransom demand or ransom payment; and

''(C) whether the threat actor operated from, or with the support or protection of, a covered foreign country.

''(b) CYBER INCIDENT INVOLVING ARTIFICIAL INTELLIGENCE.—With respect to a review under section 2251 of a covered incident that is a cyber incident involving artificial intelligence, such review shall, in addition to examining the matters described in subsection (a), also examine the following:

''(1) The capabilities of each artificial intelligence system involved in such incident, including the following:

''(A) Whether such system is proprietary, publicly available, or has publicly available model weights.

''(B) Whether such system was developed, produced, owned, or controlled by a covered foreign adversary or an entity domiciled in a covered foreign country.

''(C) Whether the safeguards of such system had been removed, disabled, or altered by a person or entity other than the developer of such system.

''(D) With respect to a system with publicly available model weights, the means by

which such model weights were distributed and the means by which such system was made available for use in the United States, including through any of the following:

''(i) Model repositories.

''(ii) Cloud service providers.

''(iii) Other hosting services.

''(2) The degree of human direction and of autonomy involved in such incident, including whether any artificial intelligence agent acted beyond the scope of the authorization granted by its developer, deployer, or user, coordinated with other artificial intelligence agents, or pursued objectives not intended by such developer, deployer, or user.

''(3) The safeguards, usage policies, monitoring, and misuse detection measures applicable to each artificial intelligence system involved in such incident, and whether such safeguards, policies, monitoring, or measures were circumvented, disabled, or ineffective.

''(4) With respect to such an incident arising during the development, training, testing, evaluation, or red teaming of an artificial intelligence system, the adequacy of the containment, isolation, network access restrictions, credential management, and

monitoring of the environment in which such development, training, testing, evaluation, or red teaming, as the case may be, occurred, the scope of any written authorization governing such development, training, testing, evaluation, or red teaming, as the case may be, and whether such incident affected any information system outside such scope, including any such environment operated by a third party on behalf of a developer or deployer of such an artificial intelligence system.

''(5) The timeliness and completeness of detection by developers and deployers, of notification to affected third parties and the Federal Government, and of public disclosures relating to such incident, whether voluntary or legally required.

''(6) Whether such incident indicates emerging artificial intelligence capabilities that have caused, or present a reasonable risk of harm to national security, homeland security, or critical infrastructure.

''(7) The use of artificial intelligence systems by defenders to detect, mitigate, and respond to such incident, and the effectiveness of such use.

''(8) Lessons for developers and deployers of artificial intelligence systems, providers of cloud com-

puting and computational resources, and network defenders.

''(9) With respect to a covered incident that involves the circumvention of the safeguards of an artificial intelligence system, whether the developer or deployer of such artificial intelligence system received notice of such circumvention before such covered incident, including from a person conducting security research in good faith, and the timeliness and adequacy of the response of such developer or deployer to such notice.

''(c) COVERED CHEMICAL, BIOLOGICAL, RADIOLOGICAL, OR NUCLEAR INCIDENTS.—With respect to a review under section 2251 of a covered incident that is a covered chemical, biological, radiological, or nuclear incident, such review shall, in addition to examining the matters described in subsection (a), also examine, in coordination with appropriate executive agencies with relevant expertise, the following:

''(1) Whether any artificial intelligence system or information system was used to seek or obtain information, planning, or technical assistance that meaningfully advanced the development, production, acquisition, or use of a chemical, biological, radiological, or nuclear weapon.

''(2) The effectiveness of safeguards intended to prevent such assistance.

''(3) The security of information systems and operational technology at facilities that possess, store, or process chemical, biological, radiological, or nuclear materials implicated by such incident.

''(d) TECHNICAL ASSISTANCE.—

''(1) REQUESTS.—The Chair may request that any person or SLTT entity the information system, operational technology, artificial intelligence system, product, or service of which were involved in a covered incident under review under section 2251 make available individuals with relevant technical or operational expertise to explain such system, technology, product, or service, as the case may be, to the NCAI Board. The provision of such assistance shall be voluntary and shall not confer any status or right of participation in such review.

''(2) REQUIREMENTS.—Technical assistance provided under paragraph (1) shall be subject to the following requirements:

''(A) Such assistance shall be provided by individuals with relevant technical or operational expertise, and no individual who occupies a legal or litigation position, or who rep-

resents a claimant or insurer, may provide such assistance.

''(B) Each individual providing such assistance shall sign a statement agreeing to comply with the procedures and confidentiality requirements of the NCAI Board.

''(C) No person or SLTT entity may publicly release information obtained through providing such assistance before the publication of the final report relating to such review without the approval of the NCAI Board, except that this subparagraph shall not restrict any disclosure required by law, regulation, or contract, any disclosure to an affected customer, insurer, counsel, or auditor, or the disclosure of information obtained independently of such assistance.

''(D) Such assistance shall be provided under the direction of the NCAI Board, and no individual providing such assistance may participate in any deliberation of the NCAI Board or in the development of any finding, recommendation, or report of the NCAI Board.

''(3) TERMINATION.—The Chair may decline or terminate technical assistance under paragraph (1)

from any person or SLTT entity that fails to comply with this subsection, and shall notify the appropriate congressional committees of any such declination or termination, as the case may be.

''(4) TREATMENT OF INFORMATION.—Information provided under this subsection shall be treated as voluntarily provided information.

''(e) COOPERATION OF EXECUTIVE AGENCIES.—

''(1) THE DEPARTMENT.—The Secretary shall ensure that each component of the Department cooperates fully and promptly with the NCAI Board, including by providing information and access to personnel requested by the NCAI Board.

''(2) OTHER EXECUTIVE AGENCIES.—The head of each executive agency shall, to the maximum extent practicable and consistent with applicable law, the protection of classified information and intelligence sources and methods, and the integrity of ongoing law enforcement investigations, provide to the NCAI Board information requested by the NCAI Board relating to a review under section 2251.

''(3) REPORTING OF NONCOOPERATION.—The NCAI Board shall include in each update required under section 2260(a) any refusal by an executive agency to provide information requested by the

NCAI Board, and any failure by an executive agency to provide such information within 30 days after the date of the request.

''(f) COORDINATION WITH LAW ENFORCEMENT AND INTELLIGENCE ACTIVITIES.—

''(1) DECONFLICTION.—The NCAI Board shall coordinate with appropriate executive agencies to ensure that a review under section 2251 does not compromise any criminal investigation or prosecution, intelligence activity, or diplomatic effort of the United States.

''(2) DEFERRAL.—Upon the written request of the head of an executive agency that states the specific reasons for such request, the NCAI Board may defer or narrow any aspect of a review under section 2251. The NCAI Board shall notify the appropriate congressional committees of each such request, and of the action taken by the NCAI Board relating thereto, not later than seven days after receiving such request, and shall reassess each such deferral or narrowing, as the case may be not less frequently than once every 90 days.

''(3) NOT A LAW ENFORCEMENT BODY.—The NCAI Board may not conduct criminal investigations. If the NCAI Board obtains information indi-

cating a Federal crime has been committed, the NCAI Board may refer such information to the appropriate executive agency, consistent with section 2258.

''(g) COORDINATION WITH OTHER INVESTIGATIVE AUTHORITIES.—The NCAI Board shall coordinate with Sector Risk Management Agencies, SLTT entities, and other executive agencies with investigative authorities to avoid duplication of effort, and may enter into memoranda of understanding with, and conduct joint reviews with, such entities. The NCAI Board may, consistent with applicable law and section 2258, exchange information with incident review bodies of the governments of allies and partners of the United States, but may not share any information obtained under this subtitle with a covered foreign adversary or an entity domiciled in a covered foreign country.

''(h) CONFIDENTIAL SUBMISSIONS.—The NCAI Board shall establish a secure mechanism through which any individual may submit information relevant to a covered incident. Except as required by law, the NCAI Board may not disclose the identity of any such individual without the consent of such individual.

''(i) ACCESS TO REPORTED INFORMATION.—

''(1) IN GENERAL.—The NCAI Board may receive and use information submitted to the Agency under subtitle D or shared with the Federal Government under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.), subject to the protections applicable to such information under such subtitle or Act, as the case may be.

''(2) LIMITATION.—In carrying out a review under section 2251, the NCAI Board shall, to the maximum extent practicable, utilize incident reports, disclosures, and technical data submitted to the Agency pursuant to subtitle D or shared under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.), as the case may be, prior to issuing requests for information or subpoenas to affected entities in order to avoid duplication of such requests or related efforts.

''(j) DRAFT REPORTS AND FACTUAL ACCURACY REVIEW.—Before adopting a final report under section 2259, the NCAI Board shall prepare a draft report of such final report. The NCAI Board shall provide to each entity the conduct of which is described in the findings of such draft report the portions of such draft report pertaining to such entity, and shall provide such entity a period of 45 days, which the NCAI Board may extend for good cause (or,

if the NCAI Board determines that an urgent threat so requires, a period of not fewer than ten days), to identify and submit to the NCAI Board factual inaccuracies in such portions and information in such portions that should be protected under section 2258. The NCAI Board shall consider any such submission but shall retain sole authority over the content of such final report. A draft report, or any portion of such a draft report, provided to an entity under this subsection shall be treated as confidential and may not be publicly disclosed by such entity, except that this subparagraph shall not restrict any disclosure required by law, regulation, or contract, any disclosure to an affected customer, insurer, counsel, or auditor, or the disclosure of information obtained independently of such assistance.

''(k) TIMELINE.—The NCAI Board shall complete each review under section 2251 and transmit a final report under section 2259 relating thereto not later than one year after the date on which such review is initiated. If the NCAI Board determines that such a review cannot be completed within such period, the NCAI Board shall notify the appropriate congressional committees of the reasons relating thereto and the anticipated date of completion, and shall update such notification not less frequently than once every 90 days until such a review is completed.

''(l) URGENT RECOMMENDATIONS.—If the NCAI Board determines at any time during a review under section 2251 that a cybersecurity threat or security vulnerability identified in the course of such review poses a risk to national security, homeland security, critical infrastructure, or public health or safety that requires immediate action, the NCAI Board shall issue urgent recommendations to appropriate entities and shall notify the appropriate congressional committees not later than 72 hours after issuing such recommendations. The NCAI Board may withhold such urgent recommendations from public release if such release would disclose a security vulnerability for which mitigations are not reasonably available.

"SEC. 2257. REQUESTS FOR INFORMATION, PRESERVATION NOTICES, AND SUBPOENAS.

''(a) REQUESTS FOR INFORMATION.—

''(1) IN GENERAL.—

''(A) AUTHORIZATION.—Except as provided in subparagraph (B), the Chair, or a designee of the Chair, may request documents, records, technical data, or testimony from any person the NCAI Board reasonably believes has information relevant to a review under section 2251, including logs, telemetry, forensic images, configuration data, internal communications,

risk assessments, and incident response documentation, and, with respect to an artificial intelligence system, system prompts, input-output pairs directly implicated in the covered incident that is the subject of such a review, artificial intelligence agent telemetry, reasoning traces, and the results of testing, evaluation, and red teaming. If the information requested relates to the information system of a customer of such a person, the Chair, or designee of the Chair, shall, where practicable, first request such information from such customer and shall notify such customer of any related subsequent request to such a person.

''(B) PROHIBITION.—The Chair, or designee of the Chair, may not request raw, proprietary internal reasoning traces, uncurated intermediate chain-of-thought activations, or pre-deployment safety red-team scratchpads created in the normal course of scientific exploration.

''(2) UNSOLICITED INFORMATION.—Any person may provide to the NCAI Board information relating to a review under section 2251 without a request under paragraph (1).

''(3) TREATMENT.—Information provided in response to a request under paragraph (1), or provided under paragraph (2), shall be treated as voluntarily provided information.

''(b) PRESERVATION NOTICES.—

''(1) AUTHORITY.—The Chair, with the approval of a majority of the full-time members of the NCAI Board, may issue a written preservation notice requiring a person to preserve documents, records, or technical data in the possession, custody, or control of such person that the NCAI Board reasonably believes are materially relevant and reasonably necessary to determine the causes or material contributing factors of a covered incident that is under review under section 2251 or under consideration for review under section 2255(d). Such a preservation notice shall, to the extent practicable, specify accounts, systems, or identifiers, rather than enterprise-wide infrastructure, to reduce undue burden and cost.

''(2) DURATION.—A preservation notice under paragraph (1) shall remain in effect for 90 days, and may be renewed for one additional period of 90 days with the approval required under such paragraph. Any further such renewal shall require such

approval and prior notice to the appropriate congressional committees.

''(3) LIMITATIONS.—A preservation notice under paragraph (1)—

''(A) shall describe the materials to be preserved with reasonable particularity;

''(B) may be satisfied by preservation of data in the format in which such data is ordinarily maintained; and

''(C) may not—

''(i) require any person subject to such a notice to—

''(I) create new records; or

''(II) disrupt normal business operations;

''(ii) require the preservation of data that is not reasonably accessible because of undue burden or cost;

''(iii) require the freezing, or suspension of continuous model training, fine-tuning, or iterative model weight updating; or

''(iv) compel the physical segregation or transfer of model weights.

''(4) MODIFICATION.—A recipient of a preservation notice under paragraph (1) may, not later

than 14 days after receipt of such notice, petition the Chair to modify such notice on the basis of undue burden, and the Chair shall respond to such petition in writing not later than 14 days after receipt of such petition.

''(5) ENFORCEMENT.—A preservation notice under paragraph (1) shall be enforceable in the same manner as a subpoena under subsection (c)(7).

''(c) SUBPOENAS.—

''(1) AUTHORITY.—The Chair may issue a subpoena to compel the production of documents, records, technical data, and other physical items, and the testimony of any person, relevant to a review under section 2251 if both of the following conditions are satisfied:

''(A) The NCAI Board has made a written request for such information to such person under subsection (a)(1), and such person has declined to provide such information or 30 days have elapsed without an adequate response, except that such period shall be ten days if the NCAI Board determines there is a substantial risk that relevant information will be lost or that an ongoing threat requires expedited action.

''(B) A majority of the full-time members of the NCAI Board approve the issuance of such subpoena in writing after considering the factors described in paragraph (2).

''(2) FACTORS.—In determining whether to approve the issuance of a subpoena under paragraph (1), the full-time members of the NCAI Board shall consider the following:

''(A) Whether the information at issue may be obtained through other means.

''(B) Whether further communication with the person at issue is likely to result in the voluntary provision of such information.

''(C) Whether a reasonable amount of time has elapsed, based on the nature of the request at issue.

''(D) The importance of such information to the review under section 2251 at issue.

''(E) Whether, after consultation with appropriate executive agencies, such subpoena would adversely affect a regulatory, law enforcement, intelligence, or diplomatic effort of the United States.

''(F) The burden on such person, including the size and resources of such person.

''(3) PART-TIME MEMBERS EXCLUDED.—Part-time members and alternate members of the NCAI Board may recommend the issuance of a subpoena under paragraph (1), but shall be excluded from deliberations and votes relating to such issuance.

''(4) REQUIREMENTS.—A subpoena issued under paragraph (1) shall be subject to the following requirements:

''(A) Such subpoena shall describe the information sought with reasonable particularity and shall provide a period for compliance of not fewer than 14 days, or not fewer than seven days in the case of expedited action described in subparagraph (A) of such paragraph.

''(B) Such subpoena may not compel the disclosure of information protected by the attorney-client privilege, the attorney work product doctrine, or any other applicable legal privilege.

''(C) Such subpoena may not compel the transfer or copy of model weights or proprietary training data from the possession of the person subject to such subpoena, but may compel remote or supervised access to an artificial intelligence system, including through supervised access within an environment controlled by such

person, to the extent necessary to evaluate the behavior of such system that is relevant to the review under section 2251 at issue. The NCAI Board shall ensure no such access or evaluation enables the extraction, derivation, or reverse-engineering of model weights or proprietary training data.

''(D) Such subpoena may not compel the production, disclosure, or inspection of proprietary source code, algorithmic architecture, or training code. The NCAI Board shall ensure such proprietary source code, algorithmic architecture, or training code is not copied, removed from any inspection environment, or ingested into any external software tool or automated model.

''(E) Such subpoena may not be issued to any department, agency, or instrumentality of the Federal Government or to an SLTT entity, or to an officer or employee of any such department, agency, instrumentality, or entity, as the case may be, with respect to matters relating to the official duties of such officer or employee.

''(F) Such subpoena may not be issued for the purpose of supporting a regulatory or enforcement action or private litigation.

''(G) An individual compelled to testify pursuant to such subpoena may be accompanied by counsel and shall be provided an opportunity to review the transcript of such testimony.

''(5) NOTICE.—Not later than seven days after the issuance of a subpoena under paragraph (1), the Chair shall notify the Secretary and the appropriate congressional committees of such issuance, including the identity of the recipient of such subpoena, a description of the information sought, and the basis for such subpoena.

''(6) PETITION TO MODIFY OR QUASH.—A person subject to a subpoena under paragraph (1) may, before the return date, petition the NCAI Board to modify or quash such subpoena. The NCAI Board shall rule on such petition in writing not later than 14 days after receipt of such petition, and the return date shall be tolled while such petition is pending.

''(7) CIVIL ACTION.—

''(A) IN GENERAL.—If a person fails to comply with a subpoena under paragraph (1) or preservation notice issued under subsection (b),

the Chair may refer such matter to the Attorney General to bring a civil action in a district court of the United States to enforce such subpoena or preservation notice, as the case may be.

''(B) VENUE.—An action under this paragraph may be brought in the judicial district in which the person against whom such action is brought resides, is found, or does business, or in the District of Columbia.

''(C) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena under paragraph (1) or preservation notice issued under subsection (b) as a contempt of court.

''(8) DELEGATION.—The authority of the Chair to issue a subpoena under paragraph (1) or preservation notice under subsection (b) may be delegated only to another full-time member of the NCAI Board.

''(9) AUTHENTICATION.—Any subpoena under paragraph (1) or preservation notice issued under subsection (b) that is issued electronically shall be authenticated with a cryptographic digital signature of the Chair or designee, or other comparable suc-

cessor technology, that allows the Chair or such designee to demonstrate that such subpoena or notice, as the case may be, was issued by the Chair or such designee and has not been altered since being so issued. Any such subpoena or notice, as the case may be, that is not so authenticated shall not be considered valid by the recipient or by any court.

''(d) STORED COMMUNICATIONS.—Nothing in this section may be construed to permit or require disclosure by a provider of a remote computing service or a provider of an electronic communication service to the public of information not otherwise permitted or required to be disclosed under chapter 121 of title 18, United States Code (commonly known as the 'Stored Communications Act').

''SEC. 2258. PROTECTION OF INFORMATION.

''(a) VOLUNTARILY PROVIDED INFORMATION.—

''(1) DISCLOSURE, RETENTION, AND USE.—Voluntarily provided information may be disclosed to, retained by, and used by the NCAI Board and any other executive agency, consistent with otherwise applicable provisions of Federal law, solely for the following purposes:

''(A) A cybersecurity purpose.

"(B) Identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability.

"(C) Responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act, a cyber incident involving terrorism, or the use of a chemical, biological, radiological, or nuclear weapon.

"(D) Responding to, investigating, prosecuting, or otherwise preventing or mitigating a serious threat to a minor, including sexual exploitation and threats to physical safety.

"(E) Preventing, investigating, disrupting, or prosecuting an offense arising out of a covered incident, or an offense listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)), except that such information may not be used under this subparagraph against the person that provided such information unless such person is suspected of having committed, conspired to commit, or aided and abetted such offense.

''(2) PROTECTIONS.—Voluntarily provided information shall be subject to the following protections:

''(A) Such information shall be considered the commercial, financial, and proprietary information of the person that provided such information when so designated by such person.

''(B) Such information shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the 'Freedom of Information Act'), and under any provision of State, local, or Tribal law requiring the disclosure of information or records.

''(C) The provision of such information shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

''(D) Such information shall not be subject to a rule of any executive agency or any judicial doctrine regarding ex parte communications with a decisionmaking official.

''(3) PROHIBITION ON REGULATORY AND ENFORCEMENT USE.—An executive agency or a SLTT entity may not use voluntarily provided information to regulate, or to take an enforcement action

against, the person that provided such information, except that such voluntarily provided information may inform the development or implementation of generally applicable guidance, standards, or regulations relating to the security of information systems.

''(4) LIABILITY PROTECTIONS.—

''(A) NO CAUSE OF ACTION.—No cause of action shall lie or be maintained in any court by any person or entity arising from the voluntary provision of information to the NCAI Board in accordance with this subtitle, and any such action shall be promptly dismissed.

''(B) EVIDENTIARY PROTECTION.—Voluntarily provided information, and any communication, document, material, or other record created for the sole purpose of preparing, drafting, or providing such information, may not be received in evidence, subject to discovery, or otherwise used in any trial, hearing, or other proceeding in or before any court, regulatory body, or other authority of the United States, a State, or a political subdivision of a State.

''(C) EXCEPTIONS.—The application of subparagraph (B) shall not—

''(i) prevent the use of voluntarily provided information to investigate or prosecute a person suspected of having committed, conspired to commit, or aided and abetted the commission of a cyber incident described in such information, if the submission itself is not disclosed; or

''(ii) create a defense to the discovery of, or otherwise affect the discovery of, any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or providing such information, or any information developed from a source independent of such voluntarily-provided information.

''(b) INFORMATION OBTAINED BY SUBPOENA.—Information obtained by subpoena under section 2257(c) shall be subject to the protections described in paragraph (2) of subsection (a), and may be disclosed to, retained by, and used by the NCAI Board and any other executive agency solely for the purposes described in paragraph (1) of such subsection. Information obtained by subpoena under section 2257(c), and information derived from such information, may not be disclosed or used to initiate or

support a civil or administrative enforcement action against the person that so obtained such information.

''(c) REPORTS OF THE NCAI BOARD.—No part of any final report of the NCAI Board under section 2259, or of any draft report under section 2256(j), relating to a covered incident or review under section 2251 may be subject to discovery, admitted into evidence or used in any civil, administrative, or State proceeding resulting from a matter included in any such report.

''(d) PRIVACY AND CIVIL LIBERTIES.—

''(1) MINIMIZATION.—The NCAI Board shall collect, retain, use, and disseminate personal information obtained under this subtitle only to the extent necessary to carry out this subtitle, and shall protect such information from unauthorized use and disclosure.

''(2) POLICIES.—Not later than 180 days after the date of the enactment of this subtitle, the Chair, in consultation with the senior official appointed under section 222 and the Officer for Civil Rights and Civil Liberties of the Department, shall establish, and publish on the website required under section 2260(e), policies governing the collection, retention, use, dissemination, and destruction of personal information and other information obtained under

this subtitle, including requirements for the return or destruction of information that is no longer necessary to carry out this subtitle.

''(e) SECURITY OF INFORMATION.—The NCAI Board shall collect, store, and protect information obtained under this subtitle in accordance with, at a minimum, the requirements for information systems categorized at the moderate impact level described in Federal Information Processing Standards Publication 199, or any successor document, and in accordance with the requirements for information systems categorized at the high impact level with respect to information relating to model weights or access to artificial intelligence systems, security vulnerabilities for which mitigations are not reasonably available, and chemical, biological, radiological, or nuclear weapons.

''(f) SECURITY VULNERABILITIES.—The NCAI Board shall coordinate with the Director, consistent with the coordinated vulnerability disclosure processes of the Agency, before publicly disclosing technical details of any security vulnerability. The NCAI Board may not publicly disclose technical details of a security vulnerability for which mitigations are not reasonably available unless the NCAI Board and the Director jointly determine that such disclosure is in the public interest.

''(g) HAZARDOUS INFORMATION.—The NCAI Board may not publicly release any information that would provide meaningful assistance in the development, production, acquisition, or use of a chemical, biological, radiological, or nuclear weapon, or detailed operational instructions for carrying out a cyber incident or circumventing the safeguards of an artificial intelligence system. The NCAI Board may include such information, as appropriate, in a classified or controlled annex to a report under section 2259.

''(h) CLASSIFIED INFORMATION.—The Secretary shall ensure that members and staff of the NCAI Board have appropriate security clearances and access to facilities necessary to receive, handle, and store classified information.

''(i) UNAUTHORIZED DISCLOSURE.—Any member, alternate member, technical advisor, staff member, or contractor of the NCAI Board, or any individual providing technical assistance under section 2256(d), who knowingly discloses information in violation of this section shall be subject to removal or disqualification from further participation in the work of the NCAI Board. The Chair shall refer any such violation to the appropriate authorities and notify the appropriate congressional committees of such violation.

''(j) DISCLOSURE TO CONGRESS.—Nothing in this subtitle may be construed to authorize the withholding of information from the appropriate congressional committees. The provision of information to such committees shall not constitute a public disclosure or a waiver of any protection under this section.

"SEC. 2259. REPORTS AND RECOMMENDATIONS.

''(a) FINAL REPORTS.—Upon the completion of a review under section 2251, the NCAI Board shall adopt, by majority vote, a final report that includes the following with respect to the covered incident that is the subject of such report:

''(1) An executive summary.

''(2) A description of the facts and timeline of such covered incident.

''(3) The root causes and contributing factors of such covered incident.

''(4) The findings of the NCAI Board, including findings regarding any act, omission, practice, or decision that caused or contributed to such covered incident.

''(5) Specific, actionable, and prioritized recommendations, and unique systemic lessons, from such covered incident, which shall identify the entity or category of entities to which such recommenda-

tion is directed, including executive agencies, SLTT entities, owners and operators of critical infrastructure, technology providers, developers and deployers of artificial intelligence systems, and Congress.

''(6) As applicable, a discussion of each aspect of such covered incident relating to artificial intelligence, terrorism, covered foreign adversaries, or chemical, biological, radiological, or nuclear weapons.

''(7) A description of any limitation on such review, including information the NCAI Board sought but was unable to obtain.

''(8) A list of the recusals disclosed under section 2254(d).

''(9) Any separate statement of a member concurring in or dissenting from such report.

''(10) Any statement submitted under subsection (d).

''(b) TECHNOLOGY NEUTRALITY.—Recommendations of the NCAI Board relating to technology solutions shall be neutral with respect to technology and vendors.

''(c) TRANSMISSION.—The Chair shall transmit each final report under this section, including any classified or controlled annex, to the Secretary, the Director, and the appropriate congressional committees on the same day.

The Secretary shall transmit each final report to the President.

''(d) STATEMENTS OF ENTITIES.—An entity to which portions of a draft report are provided under section 2256(j) may, not later than 30 days after receiving such portions, submit to the NCAI Board a written statement, subject to such reasonable length limitations as the NCAI Board may establish in accordance with the procedures developed under section 2253(a)(2)(B). If the conduct of such entity is described in the findings of the final report under section under this section, the NCAI Board shall publish such statement as an appendix to the public version of such final report, together with any response of the NCAI Board.

''(e) PUBLICATION.—

''(1) IN GENERAL.—Not later than 30 days after the transmission of a final report under subsection (c), the Secretary shall publish an unclassified version of such report on the website required under section 2260(e).

''(2) LIMITED DELAY.—The Secretary may delay publication under paragraph (1) for a period of not more than 45 days solely to complete a classification review of such report, in order to avoid compromising an ongoing law enforcement investigation,

or to allow for the mitigation of a security vulnerability. Not later than three days after any such delayed publication, the Secretary shall notify the appropriate congressional committees of the reasons relating thereto and the anticipated date of publication. Any further delay shall be subject to the same requirements and may not exceed 60 days.

''(3) REDACTIONS.—Any redaction from the public version of a final report under this section shall be limited to the purposes described in paragraph (2) and section 2258, shall be clearly marked, and may not alter any finding or recommendation. The unredacted version of such report shall be provided to the appropriate congressional committees.

''(f) RESPONSES TO RECOMMENDATIONS.—

''(1) DEPARTMENT.—Not later than 90 days after receiving a recommendation of the NCAI Board in a final report under this section, the head of each component of the Department to which such recommendation is directed shall submit to the NCAI Board and the appropriate congressional committees a written response stating whether such component accepts, accepts in part, or does not accept such recommendation, the reasons relating thereto, and, for any recommendation accepted in

whole or in part, a plan and timeline for implementation.

''(2) OTHER EXECUTIVE AGENCIES.—The NCAI Board shall transmit each recommendation in a final report under this section directed to an executive agency other than the Department to the head of such executive agency with a request for a written response within 90 days, and shall record whether such a response was received and the substance of any such response.

''(3) NON-EXECUTIVE AGENCIES.—The NCAI Board may request, and any non-executive agency may voluntarily provide, information regarding the implementation of recommendations in a final report under this section directed to such entity. Nothing in this subsection may be construed to require any such non-executive agency to implement or respond to any such recommendation.

''(g) RECOMMENDATION TRACKING.—The NCAI Board shall maintain, and update on the website required under section 2260(e) not less frequently than quarterly, a public record of each recommendation of the NCAI Board in a final report under this section, including the recipient, the date issued, each response received, and the status of implementation. The NCAI Board shall annually

designate and publish on such website a list of priority recommendations the NCAI Board determines would most improve the cybersecurity of the United States if implemented.

''(h) SUPPLEMENTAL REPORTS.—If the NCAI Board obtains new information that materially affects the findings of a final report under subsection (a), the NCAI Board may reopen the review under section 2251 that is the subject of such report and issue a supplemental report, which shall be subject to the requirements of this section. Any person may petition the NCAI Board to reconsider a finding in such initial report on the basis of new evidence, and the NCAI Board shall respond to such petition in writing not later than 90 days after receipt of such petition.

''(i) SYNTHESIS REPORTS.—Not later than two years after the date on which the NCAI Board transmits its first final report under subsection (a) and every two years thereafter, the NCAI Board shall publish a synthesis report that analyzes trends and systemic risks across reviews under section 2251 that are the subjects of such final reports and other cyber incidents, including trends relating to the following:

''(1) Cyber incidents involving artificial intelligence.

''(2) Cyber incidents involving terrorism.

''(3) Covered foreign adversary and terrorist organization activity.

''(4) Patterns of safeguard failures in artificial intelligence systems, including the following:

''(A) Failures identified through security research conducted in good faith.

''(B) Failures in artificial intelligence systems developed by entities domiciled in covered foreign countries.

''(5) The status of implementation of recommendations.

''(6) The reasons any of such recommendations have not been implemented.

"SEC. 2260. CONGRESSIONAL OVERSIGHT AND PUBLIC TRANSPARENCY.

''(a) MONTHLY UPDATES.—

''(1) IN GENERAL.—Not less frequently than once every 30 days, the Chair shall submit to the appropriate congressional committees a written update on each ongoing review under section 2251 and each cyber incident under consideration by the NCAI Board, and shall provide a briefing on such update upon the request of the chair or ranking minority member of any such committee.

''(2) CONTENTS FOR ONGOING REVIEWS.—Each update under paragraph (1) shall include, for each ongoing review under section 2251 of a covered incident, the following:

''(A) A description of such covered incident and of the affected entities and sectors.

''(B) The date on which such review was initiated, the basis for initiating such review, and any referring official.

''(C) The scope of such review and any change to such scope since the preceding update, including the reasons for any such change.

''(D) The current status of investigative activities, including the number of interviews conducted and the status of each request for information.

''(E) The identity of each person that received a request for information, the date of each such request, and whether such person complied, partially complied, or declined to comply.

''(F) Each preservation notice and subpoena issued under section 2257, the status of

compliance, any petition to modify or quash, and any referral to the Attorney General.

''(G) Any refusal or failure by an executive agency described in section 2256(e)(3).

''(H) Any request under section 2256(f)(2) to defer or narrow such review, and the action taken by the NCAI Board.

''(I) Preliminary findings and emerging observations, including any risk requiring immediate action and any urgent recommendation issued.

''(J) Whether such covered incident involves, or is suspected to involve, cyber terrorism, a covered foreign adversary, a terrorist organization, an artificial intelligence system, or a chemical, biological, radiological, or nuclear weapon.

''(K) Each member of the NCAI Board recused and each alternate member of the NCAI Board designated.

''(L) The staff and contractor resources assigned to such review and the amounts obligated for such review.

''(M) The anticipated date of completion and any change to such date.

''(N) Any obstacle to the conduct of such review, including any legal, resource, or access limitation, and any additional authority the NCAI Board determines is necessary.

''(O) Each communication recorded under section 2261(b) since the preceding update.

''(3) CONTENTS FOR INCIDENTS UNDER CONSIDERATION.—Each update under paragraph (1) shall include, for each cyber incident under consideration by the NCAI Board, a description of such cyber incident, the date on which such consideration began, and the date by which the NCAI Board expects to decide whether to initiate a review under section 2251, and, for each decision not to initiate such a review made since the preceding update, the reasons relating thereto.

''(4) FORM.—Each update under paragraph (1) shall be submitted in unclassified form but may include a classified annex.

''(5) NO WITHHOLDING ON THE BASIS OF AN ONGOING REVIEW.—The Chair and the Secretary may not decline to provide information requested by an appropriate congressional committee solely on the basis that a review under section 2251 is ongoing, that such information is predecisional, or that such

information is voluntarily provided information, but may provide such information in a classified or otherwise controlled form, as appropriate.

''(b) NOTIFICATIONS.—The Chair shall notify the appropriate congressional committees not later than seven days after, or in the case of paragraph (6), not later than 72 hours after, any of the following:

''(1) The initiation of a review under section 2251.

''(2) A decision of the NCAI Board under section 2255(d).

''(3) The issuance of a subpoena or preservation notice, or the referral of a matter to the Attorney General, under section 2257.

''(4) The appointment, removal, or resignation of a member of the NCAI Board.

''(5) The end of any period of 30 consecutive days during which the NCAI Board lacks a quorum.

''(6) The issuance of an urgent recommendation under section 2256(l).

''(7) The receipt of any communication recorded under section 2261(b) that seeks to direct, alter, suppress, or delay the selection, scope, findings, or recommendations of such a review.

''(8) Any unauthorized disclosure of information protected under section 2258.

''(c) CONSOLIDATION OF NOTICES.—A notification required under subsection (b) may be combined with any other notification to the appropriate congressional committees required under this subtitle.

''(d) BRIEFINGS ON FINAL REPORTS.—Not later than 14 days after transmitting a final report under section 2259(c), the Chair shall brief the appropriate congressional committees on such report.

''(e) PUBLIC WEBSITE.—Not later than 180 days after the date of the enactment of this subtitle, the Secretary shall establish on the public website of the Agency a dedicated page for the NCAI Board that contains the following:

''(1) Each notice of initiation published under section 2255(g), and an unclassified summary of the status of each ongoing review under section 2251, updated not less frequently than quarterly.

''(2) Each final report, supplemental report, and synthesis report under section 2259, and annual report under subsection (f), of the NCAI Board.

''(3) The proposed and final selection criteria under section 2255(f) and the public comments received on such criteria.

''(4) The conflict of interest policy under section 2254(a) and the recusal disclosures under section 2254(d).

''(5) The bylaws and procedures of the NCAI Board.

''(6) The public record of recommendations maintained under section 2259(g).

''(7) The list of declined incidents maintained under section 2255(k).

''(8) The mechanisms established under sections 2255(c) and 2256(h).

''(9) The policies established under section 2258(d)(2).

''(10) Each assessment submitted under subsection (g).

''(f) ANNUAL REPORT.—Not later than February 1 of each year, the NCAI Board shall submit to the appropriate congressional committees, and publish on the website required under subsection (e), a report that includes the following:

''(1) The reviews under section 2251 initiated, ongoing, and completed during the preceding year.

''(2) Each cyber incident considered and not selected for review during the preceding year, and the reasons relating thereto.

''(3) The number of requests for information, preservation notices, and subpoenas issued under section 2257, the rate of compliance with such requests, notices, and subpoenas, respectively, and any enforcement actions.

''(4) The number and general basis of recusals under section 2254.

''(5) The staffing and budget of the NCAI Board, and the average cost and duration of reviews.

''(6) The status of implementation of recommendations of the NCAI Board.

''(7) An assessment of the adequacy of the authorities and resources of the NCAI Board, and any recommendations for legislative changes.

''(g) PERIODIC ASSESSMENT.—Not later than three years after the date of the first meeting of the NCAI Board and every four years thereafter, the NCAI Board shall submit to the appropriate congressional committees, and publish on the website required under subsection (e), an assessment by the NCAI Board of the structure, membership, selection criteria, authorities, independence, and resources of the NCAI Board, including an assessment of whether the NCAI Board should be reconstituted as an independent establishment, and recommendations for legislative or administrative reform.

''(h) TESTIMONY.—The Chair shall testify before any appropriate committee of Congress upon request.

"SEC. 2261. INTEGRITY AND CONTINUITY OF THE NCAI BOARD.

''(a) INTEGRITY OF FINDINGS.—The selection of covered incidents for review under section 2251, the scope of each such review, and the findings, conclusions, and recommendations of the NCAI Board shall be determined by the NCAI Board. No officer or employee of the Department or of any other executive agency, other than the NCAI Board acting in accordance with this subtitle, may alter, suppress, or require the alteration of any such finding, conclusion, or recommendation of the NCAI Board, or prevent or delay the publication of any report of the NCAI Board except as provided in section 2259(e). The Secretary or the Director may submit written views on any report of the NCAI Board, which shall be published together with such report.

''(b) RECORD OF OUTSIDE COMMUNICATIONS.—The NCAI Board shall maintain a record of each communication received by any member or staff of the NCAI Board from any individual who is not a member or staff of the NCAI Board that seeks to influence the selection of a covered incident for review under section 2251, or the scope, conduct, findings, or recommendations of such a review,

including the date of such communication, the identity and affiliation of such individual, and a summary of such communication. This subsection shall not apply to information provided through the procedures established under this subtitle, including technical assistance under section 2256(d), responses to requests for information under section 2257, submissions under section 2256(j), and referrals under section 2255(b).

''(c) CONTINUITY.—

''(1) IN GENERAL.—The NCAI Board may not be abolished, suspended, or consolidated, and the functions of the NCAI Board may not be transferred, except as expressly provided by an Act of Congress enacted after the date of the enactment of this subtitle.

''(2) LOSS OF QUORUM.—If the NCAI Board lacks a quorum for 60 consecutive days, the Secretary shall, not later than seven days after the 60th such day, submit to the appropriate congressional committees a plan and timeline to restore a quorum. During any period in which the NCAI Board lacks a quorum, the staff of the NCAI Board shall continue to preserve evidence, maintain the records of ongoing reviews, and carry out such other functions as do not require action by the NCAI Board, and

each deadline applicable to an ongoing review under this subtitle shall be tolled.

''(3) ONGOING REVIEWS.—The termination of the service of any member of the NCAI Board shall not terminate any review under section 2251.

''SEC. 2262. RULES OF CONSTRUCTION.

''Nothing in this subtitle may be construed to—

''(1) authorize the NCAI Board to regulate any person or to require any person to report a cyber incident;

''(2) modify or limit subtitle D, section 2233, or the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.), or any protection applicable to information submitted or shared under such provisions;

''(3) limit the authority of any executive agency with respect to law enforcement, intelligence, counterintelligence, or military activities;

''(4) establish a private right of action, or create any right or benefit, substantive or procedural, enforceable at law or in equity by any person against the United States, including with respect to the selection of, or a decision to not so select, a covered incident for review under section 2251;

''(5) modify, limit, or preempt the terms of any voluntary public-private partnership, commitment, industry-led safety consortium, or independent pre-deployment safety evaluation regime entered into with the Federal Government by artificial intelligence developers;

''(6) authorize the interception of communications, the acquisition of the contents of communications, or any other collection of information not otherwise authorized by law;

''(7) authorize the NCAI Board to review, make findings regarding, or make recommendations regarding the content of lawful speech, including information characterized as misinformation, disinformation, or malinformation, or any other activity protected by the First Amendment to the Constitution of the United States;

''(8) discourage or penalize security research conducted in good faith, authorized testing, evaluation, or red teaming of information systems or artificial intelligence systems, including such testing performed by or with artificial intelligence systems or artificial intelligence agents, the development or provision of lawful security testing tools, or the disclosure of security vulnerabilities in good faith;

''(9) limit the access of Congress to any information; or

''(10) authorize the NCAI Board to establish, prescribe, or enforce mandatory design, development, alignment, or safety standard for artificial intelligence systems or artificial intelligence models.

''SEC. 2263. AUTHORIZATION OF APPROPRIATIONS.

''There are authorized to be appropriated such sums as may be necessary to carry out this subtitle for each of fiscal years 2027 through 2031.

''SEC. 2264. DEFINITIONS.

''In this subtitle:

''(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term 'appropriate congressional committees' means—

''(A) the Committee on Homeland Security of the House of Representatives; and

''(B) the Committee on Homeland Security and Governmental Affairs of the Senate.

''(2) ARTIFICIAL INTELLIGENCE.—The term 'artificial intelligence' has the meaning given such term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

''(3) ARTIFICIAL INTELLIGENCE AGENT.—

''(A) IN GENERAL.—The term 'artificial intelligence agent' means a software-based system, including any such system that is created, instantiated, or directed by another artificial intelligence agent, that—

''(i) uses an artificial intelligence model to perceive, reason, plan, or make decisions;

''(ii) autonomously takes actions or interacts with other software systems, information systems, digital services, users, physical or virtual environments, or other artificial intelligence agents, including by executing code, invoking tools, or using credentials, whether on behalf of a person or organization or outside the scope of any authorization granted by the developer, deployer, or operator of such system; and

''(iii) operates with no meaningful real-time human capability to intervene, review, or revoke execution steps.

''(B) EXCLUSION.—The term 'artificial intelligence agent' does not include routine deterministic automation, scripted software tasks, search indexing, or standard conversational as-

sistants that require continuous human prompt-and-response interactions.

''(4) ARTIFICIAL INTELLIGENCE MODEL.—The term 'artificial intelligence model' means a component of an artificial intelligence system that is derived using mathematical, computational, statistical, or machine learning techniques and that is used to produce outputs from a given set of inputs.

''(5) ARTIFICIAL INTELLIGENCE SYSTEM.—The term 'artificial intelligence system' means any of the following:

''(A) Artificial intelligence.

''(B) A system, software, hardware, model, tool, or other utility that operates in whole or in part through the utilization of artificial intelligence, including an artificial intelligence agent.

''(6) CHAIR.—The term 'Chair' means the Chair of the NCAI Board designated under section 2253.

''(7) CHEMICAL, BIOLOGICAL, RADIOLOGICAL, OR NUCLEAR WEAPON.—The term 'chemical, biological, radiological, or nuclear weapon' means—

''(A) with respect to a chemical, biological, or radiological weapon, a weapon described in

subparagraph (B), (C), or (D), respectively, of section 2332a(c)(2) of title 18, United States Code; or

''(B) with respect to a nuclear weapon, a nuclear explosive device.

''(8) COVERED CHEMICAL, BIOLOGICAL, RADIOLOGICAL, OR NUCLEAR INCIDENT.—

''(A) IN GENERAL.—The term 'covered chemical, biological, radiological, or nuclear incident' means a cyber incident that involves any of the following:

''(i) The use of an information system or artificial intelligence system to seek or obtain information, planning, or technical assistance that meaningfully advances, or could meaningfully advance, the development, production, acquisition, or use of a chemical, biological, radiological, or nuclear weapon.

''(ii) The compromise or attempted compromise of an information system or operational technology at a facility that possesses, stores, or processes materials that could be used to develop, produce, or use a chemical, biological, radiological, or

nuclear weapon, if such compromise could result in the release, theft, or diversion of such materials.

''(iii) The circumvention of safeguards of an artificial intelligence system that are intended to prevent assistance with the development, production, acquisition, or use of a chemical, biological, radiological, or nuclear weapon.

''(iv) The unauthorized acquisition of sensitive information relating to a chemical, biological, radiological, or nuclear weapon or to the security of materials described in clause (ii).

''(B) EXCLUSION.—The term 'covered chemical, biological, radiological, or nuclear incident' does not include security research conducted in good faith or authorized testing, evaluation, or red teaming of an information system or artificial intelligence system.

''(9) COVERED FOREIGN ADVERSARY.—The term 'covered foreign adversary' means—

''(A) any foreign government, military, intelligence service, or other authority of a covered foreign country acting independently; or

''(B) any organization, group, or person acting on behalf of, with the support, direction, control, or influence of, or trained or supplied by, such a foreign government, military, intelligence service, or other authority, as the case may be, including any proxy, militia, paramilitary organization, intelligence or security service, or other state-sponsored actor that receives material support, training, technical assistance, or operational coordination from a covered foreign country and engages in activities that threaten the national security of the United States or its allies.

''(10) COVERED FOREIGN COUNTRY.—The term 'covered foreign country' means a country that—

''(A) the intelligence community has identified as a foreign adversary in its most recent Annual Threat Assessment; or

''(B) the Secretary, in coordination with the Director of National Intelligence, has identified as a foreign adversary that is not included in such Annual Threat Assessment.

''(11) COVERED INCIDENT.—The term 'covered incident' means an incident the NCAI Board determines, based on specific criteria, has caused, or pre-

sents a substantial or demonstrable risk of, harm to national security, economic security, public health or safety, or the operation of critical infrastructure, including any of the following:

''(A) A significant cyber incident.

''(B) A cyber incident involving terrorism.

''(C) A covered chemical, biological, radiological, or nuclear incident.

''(D) A cyber incident involving artificial intelligence that the NCAI Board determines, in accordance with the criteria established under section 2255(f), is of sufficient severity, novelty, or national significance to warrant review.

''(E) A significant cyber disruption.

''(F) A cyber incident that is part of a campaign by a covered foreign adversary to gain or maintain access to critical infrastructure for the purpose of future disruption or destruction.

''(G) A group of related cyber incidents, including a campaign by a threat actor, that includes an incident or disruption, as the case may be, described in any of subparagraphs (A) through (E).

''(12) CYBER INCIDENT.—The term 'cyber incident' has the meaning given such term in paragraph (5) of section 2240, except that for purposes of this subtitle, subparagraph (B) of such paragraph shall not apply.

''(13) CYBER INCIDENT INVOLVING ARTIFICIAL INTELLIGENCE.—

''(A) IN GENERAL.—The term 'cyber incident involving artificial intelligence' means a cyber incident resulting in, or reasonably likely to result in, harm to national security, economic security, public health or safety, or the operation of critical infrastructure in which any of the following occurred:

''(i) An artificial intelligence system was used to plan, develop, automate, scale, or carry out any part of such cyber incident.

''(ii) An artificial intelligence system, including an artificial intelligence agent, acted without the authorization of the developer, deployer, or operator of such system to access or affect an information system, including during the development,

training, testing, evaluation, or deployment of such system.

''(iii) An artificial intelligence system, including the model weights, training or evaluation infrastructure, or safeguards of such system, was a target of such cyber incident.

''(iv) An artificial intelligence system was subjected to sustained, automated model extraction attacks by a covered foreign adversary, resulting in the confirmed exfiltration of proprietary model weights.

''(B) EXCLUSION.—The term 'cyber incident involving artificial intelligence' does not include any of the following:

''(i) Security research conducted in good faith, or authorized testing, evaluation, or red teaming of an information system or artificial intelligence system, including any such research, testing, evaluation, or red teaming conducted using an artificial intelligence agent, to the extent such research, testing, evaluation, or red teaming remains within the scope of such

good faith conditionality or authorization, as the case may be.

''(ii) Conduct occurring within authorized testing, evaluation, or red teaming conducted under appropriate technical and operational controls, unless such conduct causes harm to national security, economic security, public health or safety, or the operation of critical infrastructure.

''(iii) A deviation from instructions or attempted unauthorized action, unless such deviation or action causes harm to national security, economic security, publish health or safety, or the operation of critical infrastructure[.

''(14) CYBER INCIDENT INVOLVING TERRORISM.—

''(A) IN GENERAL.—The term 'cyber incident involving terrorism' means a cyber incident that—

''(i) is carried out by, or on behalf of, a terrorist organization; or

''(ii) constitutes terrorism, without regard to whether an artificial intelligence system carried out any part of such cyber

incident with limited or no contemporaneous human direction, except that the intent described in section 2(18)(B) shall be determined with respect to the person who directed, deployed, or otherwise caused the use of such system.

''(B) EXCLUSIONS.—The term 'cyber incident involving terrorism' does not include any of the following:

''(i) Any activity carried out by or on behalf of, and with the authorization of, the United States Government, a State, or a unit of local government, including activity carried out by a contractor acting within the scope of such authorization.

''(ii) Security research conducted in good faith, or authorized testing, evaluation, or red teaming, of an information system or artificial intelligence system.

''(iii) Any activity protected by the First Amendment to the Constitution of the United States, including advocacy, protest, or dissent.

''(15) DEPLOYER.—The term 'deployer' means, with respect to an artificial intelligence system, any

person or other entity that makes such artificial intelligence system available for use by others, including through an application, product, service, or application programming interface, or that uses such artificial intelligence system, including an artificial intelligence agent, in the operation of an information system, other than an individual who uses such artificial intelligence system solely for personal purposes.

''(16) DEVELOPER.—

''(A) IN GENERAL.—The term 'developer' means, with respect to an artificial intelligence system or artificial intelligence model, any person or other entity that designs, trains, or substantially modifies such system or model, as the case may be, including by fine-tuning such system or model, as the case may be, or by removing, disabling, or altering the safeguards of such system or model, as the case may be.

''(B) APPLICATION.—The term 'developer' applies without regard to whether the artificial intelligence system or artificial intelligence model at issue is proprietary or has publicly available model weights, the size of the person or other entity at issue, or whether such person

or entity is organized under the laws of, or located in, the United States or a foreign country, including a covered foreign country.

"(C) MODIFICATIONS.—

"(i) IN GENERAL.—A person or other entity that substantially modifies an artificial intelligence system or artificial intelligence model developed by another person or entity shall satisfy the definition of the term 'developer' only with respect to such modification.

"(ii) EXCLUSION.—Substantial modifications under clause (i) do not include building applications, prompts, or orchestration from a third-party artificial intelligence model.

"(17) FULL-TIME MEMBER.—The term 'full-time member' means a member of the NCAI Board appointed under section 2252(a)(1).

"(18) MODEL WEIGHTS.—The term 'model weights' means the numerical parameters, including biases and other learned parameters, of an artificial intelligence model that are derived through training and that, in combination with the architecture of

such model, are sufficient to enable the functioning of such model.

''(19) PART-TIME MEMBER.—The term 'part-time member' means a member of the NCAI Board appointed under section 2252(a)(2).

''(20) PERSON.—The term 'person' means an individual, partnership, corporation, association, organization, or other nongovernmental entity.

''(21) REVIEW.—The term 'review' means a review of a covered incident conducted by the NCAI Board under this subtitle.

''(22) SIGNIFICANT CYBER DISRUPTION.—

''(A) IN GENERAL.—The term 'significant cyber disruption' means an event not caused by malicious activity, including a defective software update, a configuration error, or a failure of an artificial intelligence system, that causes a disruption of an information system or operational technology that the NCAI Board determines is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the people of the United States.

''(B) EXCLUSION.—The term 'significant cyber disruption' does not include security research conducted in good faith, or authorized testing, evaluation, or red teaming, of an information system or artificial intelligence system, including any such research, testing, evaluation, or red teaming conducted using an artificial intelligence agent, to the extent such research, testing, evaluation, or red teaming remains within the scope of such good faith conditionality or authorization, as the case may be, and is not likely to result in demonstrable harm described in subparagraph (A).

''(23) SIGNIFICANT CYBER INCIDENT.—The term 'significant cyber incident' has the meaning given such term in section 2240, except that, for purposes of this subtitle, the determination described in such section may be made by the Secretary or by the NCAI Board.

''(24) TERRORIST ORGANIZATION.—The term 'terrorist organization' means—

''(A) any entity designated as a foreign terrorist organization pursuant to section 219 of the Immigration and Nationality Act (8 U.S.C. 1189); or

''(B) any entity engaged in terrorism.

''(25) VOLUNTARILY PROVIDED INFORMATION.—

''(A) IN GENERAL.—The term 'voluntarily provided information' means information, including documents, records, technical data, and testimony, provided to the NCAI Board under section 2257 other than pursuant to a subpoena issued under subsection (c) of such section 2257, including information provided in response to a request under subsection (a) of such section 2257, technical assistance provided under subsection (d) of section 2256, and information submitted under subsection (h) of such section 2256.

''(B) EXCEPTION.—The term 'voluntarily provided information' does not include information submitted to the Agency under subtitle D or shared under the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501 et seq.), which shall remain subject to the protections applicable to such information under such subtitle or Act, as the case may be.''.

SEC. 3. IMPLEMENTATION AND TRANSITION.

(a) INITIAL APPOINTMENTS.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Homeland Security shall appoint the members of the National Cyber and AI Investigations NCAI Board established under section 2251 of the Homeland Security Act of 2002, as added by section 2 (in this section referred to as the ''NCAI Board''), and designate the Chair and Vice Chair of such NCAI Board.

(b) FIRST MEETING.—The NCAI Board shall hold its first meeting not later than 30 days after the date on which a majority of the members of the NCAI Board have been appointed.

(c) INTERIM SUPPORT.—Until amounts are first appropriated pursuant to the authorization of appropriations under section 2263 of the Homeland Security Act of 2002, as added by section 2, the Director of the Cybersecurity and Infrastructure Security Agency shall provide the NCAI Board with staff and resources necessary to carry out subtitle E of title XXII of such Act, as added by such section 2, from amounts otherwise available to the Director. Not later than 30 days after the date of the enactment of this Act, the Director shall notify the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate of the staff and resources to be so

provided and any functions of the Agency that will be reduced or reassigned as a result of such provision.

SEC. 4. CLERICAL AMENDMENT.

The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended by inserting after the item relating to section 2246 the following new items:

''Subtitle E—National Cyber and AI Investigations Board

''Sec. 2251. Establishment, mission, and organization.
''Sec. 2252. Membership.
''Sec. 2253. Chair, Executive Director, and staff.
''Sec. 2254. Ethics, conflicts of interest, and recusal.
''Sec. 2255. Selection of covered incidents for review.
''Sec. 2256. Conduct of reviews.
''Sec. 2257. Requests for information, preservation notices, and subpoenas.
''Sec. 2258. Protection of information.
''Sec. 2259. Reports and recommendations.
''Sec. 2260. Congressional oversight and public transparency.
''Sec. 2261. Integrity and continuity of the NCAI Board.
''Sec. 2262. Rules of construction.
''Sec. 2263. Authorization of appropriations.
''Sec. 2264. Definitions.''.''.