119TH CONGRESS
2D SESSION

S. _____

To establish the Cybersecurity and AI Board of Investigations, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MARKEY introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To establish the Cybersecurity and AI Board of Investigations, 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 ''Cybersecurity and AI Board of Investigations Act of 2026''.

SEC. 2. FINDINGS; PURPOSE.

(a) FINDINGS.—Congress finds the following:

(1) Robust cybersecurity infrastructure and institutions are integral to national security and economic security.

(2) Cyber threats have become more pervasive and potentially more disruptive with continued digitization across economic sectors.

(3) The advancement and increased accessibility of artificial intelligence can strengthen cybersecurity controls while also increasing the volume and sophistication of cyber threats.

(4) Critical infrastructure sectors, such as clean and wastewater utilities and telecommunications networks, are susceptible to artificial intelligence-enabled cyber incidents.

(5) As artificial intelligence systems continue to evolve, these trends in cybersecurity threats will accelerate.

(6) Other emerging technologies, including quantum computing, are likely to pose additional, novel cybersecurity threats that will compound on artificial intelligence-driven risks.

(7) The Federal Government has an interest in understanding cyber incidents in this shifting threat landscape and advancing best practices in cybersecurity.

(b) PURPOSE.—The purposes of this Act are—

(1) to establish the Cybersecurity and AI Board of Investigations; and

(2) to bolster the cyber defenses of public and private institutions in responding to the cyber risks posed by artificial intelligence and other emerging technologies.

SEC. 3. CYBERSECURITY AND AI BOARD OF INVESTIGATIONS.

(a) DEFINITIONS.—In this section:

(1) ARTIFICIAL INTELLIGENCE.—The term ''artificial intelligence'' has the meaning given the term in section 238(g) of the National Defense Authorization Act for Fiscal Year 2019 (10 U.S.C. note prec. 4061; Public Law 115–232).

(2) BOARD.—The term ''Board'' means the Cybersecurity and AI Board of Investigations established under subsection (b)(1).

(3) CHAIR.—The term ''Chair'' means the Chair of the Board designated under subsection (c)(3)(A)(i).

(4) CYBERSECURITY PURPOSE; CYBERSECURITY THREAT; INFORMATION SYSTEM; SECURITY CONTROL; SECURITY VULNERABILITY.—The terms ''cybersecurity purpose'', ''cybersecurity threat'', ''information system'', ''security control'', and ''security vulnerability'' have the meanings given those terms

in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(5) FEDERAL AGENCY.—The term ''Federal agency'' means any executive department, military department, Government-controlled corporation, or other establishment in the executive branch of the Federal Government, including the Executive Office of the President or any independent regulatory agency.

(6) FEDERAL CIVILIAN EXECUTIVE BRANCH AGENCY.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''Federal civilian executive branch agency'' means a Federal agency.

(B) EXCEPTION.—The term ''Federal civilian executive branch agency'' does not include the Department of Defense or any Federal agency that is an element of the intelligence community, as defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(7) FEDERAL CIVILIAN EXECUTIVE BRANCH INFORMATION SYSTEM.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term ''Federal civilian executive branch information system'' means any information system operated by a Federal civilian executive branch agency.

(B) EXCEPTION.—The term ''Federal civilian executive branch information system'' does not include—

(i) a national security system, as defined in section 3552(b) of title 44, United States Code; or

(ii) a system described in paragraph (2) or (3) of section 3553(e) of title 44, United States Code.

(8) INCIDENT.—The term ''incident'' means an occurrence that actually or imminently jeopardizes, without lawful authority—

(A) the integrity, confidentiality, or availability of information on an information system; or

(B) an information system.

(9) NEAR-MISS.—The term ''near-miss'' means a circumstance—

(A) in which a known or newly discovered security vulnerability is exploited in an attempt

to jeopardize the integrity, confidentiality, or availability of information on an information system; and

(B) through which no harm amounting to a significant cyber incident, as defined by the Board, is realized.

(10) RELEVANT CONGRESSIONAL COMMITTEES.—The term ''relevant congressional committees'' means—

(A) the Committee on Commerce, Science, and Transportation of the Senate;

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

(C) the Committee on Energy and Commerce of the House of Representatives; and

(D) the Committee on Homeland Security of the House of Representatives.

(b) ESTABLISHMENT; PURPOSES; ORGANIZATION.—

(1) ESTABLISHMENT.—On the date that is 90 days after the date of enactment of this Act, there is established as an independent establishment, as defined in section 104 of title 5, United States Code, the Cybersecurity and AI Board of Investigations.

(2) CHARTER.—The Board established under paragraph (1) shall establish a charter, which shall

be made publicly available, that includes non-exhaustive criteria for, and inform the prioritization of, the work of the Board, including—

(A) initiating reviews and assessments of incidents;

(B) conducting trend analyses;

(C) placing a limitation on incidents eligible for review to incidents for which all evidence, factual findings, and recommendations are unclassified or declassified to the best knowledge of the Board at the time of selection.

(3) PURPOSES.—The purposes of the Board are to—

(A) advance the safety, reliability, and resilience of the digital and communications infrastructure of the United States, which supports commerce, innovation, and public safety;

(B) conduct independent and impartial reviews and assessments with respect to—

(i) incidents affecting Federal civilian executive branch information systems or non-Federal information systems, particularly such systems that support critical infrastructure sectors;

(ii) near-misses in which a significant cybersecurity incident was narrowly averted;

(iii) systemic cybersecurity vulnerabilities across sectors, vendors, or technology categories, including within the artificial intelligence sector, that give rise to incidents affecting relevant Federal civilian executive branch and non-Federal information systems; and

(iv) breakdowns in regulatory oversight, coordination, or response processes with respect to incidents and systemic risks affecting critical infrastructure sectors;

(C) identify contributing technical, organizational, and systemic failures relating to each review and assessment conducted under subparagraph (B) in order to produce actionable recommendations for implicated public and private entities on improving the resilience of the United States with respect to cybersecurity threats and security vulnerabilities;

(D) in coordination with the Director of the National Institute of Standards and Tech-

nology and the Assistant Secretary of Commerce for Communications and Information, establish and maintain the near-miss system established under paragraph (4) to collect and analyze confidential reports of incidents and near-misses from public and private entities for the purpose of improving the resilience of the United States with respect to security vulnerabilities;

(E) facilitate learning and transparency across the public and private sectors by publicly releasing timely reports of the reviews and assessments conducted under subparagraph (B);

(F) issue trend analyses with respect to recurring cybersecurity threats, security vulnerabilities, and systemic risk patterns, with attention paid to the novel and intensified risks relating to the continued development and adoption of artificial intelligence;

(G) maintain a historical record of major incidents and contributing risk patterns with respect to those major incidents to promote the proactive reduction of cybersecurity threats and security vulnerabilities across critical infrastructure sectors; and

(H) operate independently from regulatory review and enforcement actions without assigning legal fault or liability for any review and assessment conducted under subparagraph (B).

(4) OFFICES, BUREAUS, AND DIVISIONS OF THE BOARD.—The Board shall establish such distinct and appropriately staffed offices, bureaus, and divisions as may be necessary to carry out this section and investigate and report on incidents, which shall include the following:

(A) The Office of Investigations, which shall be responsible for—

(i) conducting investigations into significant incidents, failures of information systems, intrusions into information systems, and near-misses;

(ii) developing the factual record necessary for the Board to determine the causes of, and contributing factors to, the matters described in clause (i); and

(iii) supporting the development of reports, findings, and recommendations of the Board under this section.

(B) The Office of Trend Analysis and Learning, which shall be responsible for—

(i) administering the near-miss reporting system established under paragraph (5), which may inform wider trend analyses;

(ii) issuing public trend reports to promote proactive reduction of cybersecurity threats and security vulnerabilities across critical infrastructure sectors; and

(iii) conducting ongoing analysis of the novel and intensifying cybersecurity risks posed by emerging technologies, including artificial intelligence.

(C)(i) The Office of Coordination, which shall be responsible for—

(I) serving as the principal liaison between the Board and Federal agencies, including for the purpose of facilitating secure information sharing and coordination during investigations conducted by the Board;

(II) serving as the principal liaison between the Board and private sector entities; and

(III) coordinating with the Office of Investigations to ensure timely and effi-

cient access to relevant Federal, State, local, and private sector personnel, systems, and information for the purposes of an investigation conducted by the Board.

(ii) The Office of Coordination shall establish separate internal functional units, as appropriate, to manage coordination with Federal entities and coordination with private sector entities, respectively, in order to ensure clear channels of communication and preserve the independence of investigative activities conducted by the Board.

(5) VOLUNTARY NEAR-MISS REPORTING SYSTEM.—The Board shall establish a voluntary, anonymized near-miss reporting system, which shall—

(A) allow individuals and organizations to confidentially report near-misses within critical infrastructure sectors, including events that could have disrupted critical communications or commerce systems or exposed private data;

(B) protect from disclosure the identity of each individual or organization submitting a report under subparagraph (A);

(C) be designed to identify systemic security vulnerabilities across technologies, sectors, and governance models; and

(D) support proactive risk management and learning without attribution of fault or liability.

(c) MEMBERSHIP.—

(1) BOARD MEMBERS.—

(A) IN GENERAL.—The Board shall be composed of 5 members, each of whom shall be appointed—

(i) by the President, by and with the advice and consent of the Senate; and

(ii) on the basis of technical qualification, professional standing, and demonstrated knowledge in cybersecurity or related fields.

(B) LIMITATION.—Not more than 3 members of the Board may be members of the same political party.

(2) TERMS OF OFFICE AND REMOVAL.—

(A) IN GENERAL.—Each member of the Board shall hold office for a term of 5 years.

(B) VACANCIES.—A member of the Board appointed to fill a vacancy occurring before the

expiration of the term for which the predecessor of that member was appointed shall be appointed for the remainder of that term.

(C) END OF TERM.—When the term of office of a member of the Board ends, the member may continue to serve until a successor is appointed pursuant to paragraph (1)(A).

(D) REMOVAL.—The President may remove a member of the Board for inefficiency, neglect of duty, or malfeasance in office.

(E) PAY.—Each member of the Board shall be paid an annual rate of basic pay not to exceed the rate paid for a position at level IV of the Executive Schedule under section 5315 of title 5, United States Code.

(3) CHAIR AND VICE CHAIR.—

(A) CHAIR.—

(i) IN GENERAL.—The President shall designate, by and with the advice and consent of the Senate, a Chair of the Board.

(ii) DUTIES AND POWERS.—The Chair shall—

(I) serve as the chief executive and administrative officer of the Board; and

(II) subject to the general policies and decisions of the Board—

(aa) appoint and supervise officers and employees, other than regular and full-time employees of the offices of other members of the Board, necessary to carry out this section;

(bb) fix the pay of officers and employees who are appointed to carry out this section;

(cc) distribute business among the officers, employees, and administrative units of the Board; and

(dd) supervise the expenditures of the Board.

(B) VICE CHAIR.—The President shall designate a Vice Chair of the Board, by and with the advice and consent of the Senate.

(C) TERMS.—The Chair and Vice Chair shall each hold office for a term of 3 years.

(D) VACANCY.—When the Chair is absent or unable to serve, or when the position of

Chair is vacant, the Vice Chair shall serve as Chair.

(4) PERSONNEL MATTERS.—

(A) IN GENERAL.—Subject to subparagraph (B), each member of the Board shall appoint and supervise employees in the office of that member, provided that each such employee has been approved for employment with the Board by the designated agency ethics official with respect to the Board under the same guidelines that apply to all employees of the Board.

(B) LIMITATION.—Except with respect to the office of the Chair of the Board, the authority under subparagraph (A) shall be limited to the number of full-time equivalent positions (plus 1 senior professional position, the annual rate of basic pay of which shall be not greater than that for step 10 of grade 15 of the General Schedule), as allocated annually by the Chair of the Board through the internal staffing plan of the Board.

(d) CONVENING THE BOARD.—

(1) IN GENERAL.—The Board—

(A) shall meet not fewer than 4 times each calendar year at a time and date to be determined by the Chair; and

(B) may meet at additional times at the call of the Chair.

(2) QUORUM.—Three members of the Board shall constitute a quorum for conducting the business of the Board.

(e) REVIEW AND ASSESSMENT; REPORTS.—

(1) INITIATION OF REVIEW.—The Board may initiate a review and assessment described in subsection (b)(2)(B) upon a majority vote of all members of the Board, the results of which shall be made publicly available.

(2) COMMENCEMENT OF REVIEW AND ASSESSMENT.—In addition to a meeting of the Board convened under subsection (d), the Chair may, at any time, call a meeting of the Board to initiate a review and assessment described in subsection (b)(3)(B).

(3) REPORTS.—Upon completing each review and assessment described in subsection (b)(3)(B), the Board shall prepare a report with respect to the event that is the subject of the review and assessment that—

(A) contains factual findings and actionable recommendations for improving cybersecurity practices, systemic resilience, incident response practices and policies, and coordination across public and private entities;

(B) includes—

(i) a timeline of relevant events;

(ii) an analysis of contributing technical, organizational, and systemic factors with respect to the applicable event;

(iii) a section relating to insights and lessons learned that—

(I) identifies—

(aa) factors that enhanced or impeded the review and assessment by the Board; and

(bb) any gaps in authorities, tools, or interagency coordination; and

(II) contains recommendations to improve the future operations of the Board;

(iv) appendices that include—

(I) technical indicators of compromise, such as data points or arti-

facts that identify or describe the methods used in an incident; and

(II) detailed methodological information with respect to the analytical processes, tools, and technical methods used to conduct each review and assessment described in subsection (b)(3)(B); and

(v) a plain language executive summary of the matters described in this paragraph, which shall be accessible to a non-technical audience; and

(C) is informed by and composed of only unclassified or declassified information and information appropriate for public consumption.

(4) UPDATES.—The insights and lessons learned described in paragraph (3)(B)(iii) shall—

(A) inform updates to Board procedures, training, and coordination protocols; and

(B) be shared across the Federal cybersecurity ecosystem to improve interagency readiness.

(5) PUBLIC AVAILABILITY.—The Board shall—

(A) submit to the relevant congressional committees each report prepared under para-

graph (3), consistent with the protections for documents and testimony voluntarily provided to the Board under subsection (i)(2); and

(B) make each report prepared under paragraph (3) publicly available, consistent with the protections for documents and testimony voluntarily provided to the Board under subsection (i)(2).

(6) RESPONSES.—Not later than 90 days after the date on which the Board issues a report prepared under paragraph (3) that includes a recommendation applying to a Federal civilian executive branch agency, each such Federal civilian executive branch agency shall respond in writing to that recommendation, even when the Federal civilian executive branch agency does not follow the recommended course of action, to allow the Board to track the progress of implementation across all of the recommendations of the Board.

(f) PERSONNEL.—

(1) IN GENERAL.—The Board shall be supported by a permanent, full-time Federal staff, which may include positions as—

(A) lead investigators;

(B) malware analysts;

(C) system engineers;

(D) legal counsel;

(E) digital forensic experts;

(F) communications professionals and technical writers; and

(G) other subject matter experts, as determined necessary by the Chair.

(2) ADDITIONAL STAFF.—In addition to the staff described in paragraph (1), a member of the Board may nominate personal support staff to assist in the work of the Board, subject to applicable background checks, security clearances, and financial disclosure requirements.

(3) PERSONNEL FLEXIBILITY.—To increase the capabilities of the Board, the Board may—

(A) enter into agreements with federally funded research and development centers;

(B) appoint special Government employees, as defined in section 202(a) of title 18, United States Code; and

(C) as necessary, contract with private sector or academic experts to serve as investigators.

(g) EXEMPTION FROM CERTAIN LAWS.—The Board shall not be subject to—

(1) chapter 10 of title 5, United States Code (commonly known as the ''Federal Advisory Committee Act''); or

(2) section 552b of title 5, United States Code (commonly known as the ''Government in the Sunshine Act'').

(h) BOARD MANAGEMENT.—

(1) IN GENERAL.—To ensure that the Board fulfills the purposes described in subsection (b)(3), the Chair shall take all necessary actions to manage the affairs of the Board and the conduct of the reviews and assessments described in subsection (b)(3)(B), which shall include—

(A) developing and promulgating, with the approval of the Board, a charter and other bylaws and internal procedures concerning the work of the Board, including non-exhaustive criteria for defining a significant cybersecurity incident and selecting incidents for investigation, all of which shall be made public; and

(B) making contracts and entering into agreements with Federal departments and Federal agencies as necessary and appropriate to carry out the responsibilities of the Board, including by coordinating with the Secretary of

Commerce, the Director of the National Institute of Standards and Technology, and the Assistant Secretary of Commerce for Communications and Information.

(2) PARTY SYSTEM.—

(A) IN GENERAL.—The Chair may adopt a party participation system under which an organization affected by a matter that is subject to a review and assessment described in subsection (b)(3)(B), including any entity operating or providing digital communications, technology products, or critical infrastructure services implicated in that matter, may provide factual input for investigators of the Board.

(B) LEVEL OF PARTICIPATION.—A party that provides factual input under subparagraph (A) may not participate in drafting findings or shaping recommendations contained in, or reviewing, a final report of the Board before publication of that report.

(3) CONFLICTS OF INTEREST.—The Chair shall implement a system to identify, mitigate, and manage any conflicts of interest that may arise as a result of participation by an individual in the work of the Board under this section.

(i) REQUESTS FOR INFORMATION AND ADMINISTRATIVE SUBPOENAS.—

(1) PURPOSE.—In order to ensure that the Board has sufficient information to conduct the reviews and assessments required under subsection (e) and issue reports under that subsection, the Chair, or an appropriate designee of the Chair, may request and receive relevant documents (including in electronic form) and testimony from, and issue subpoenas ad testificandum and subpoenas duces tecum to—

(A) any entity or individual affected by the incident or issue giving rise to a review and assessment under subsection (e);

(B) any entity that, or individual who, responded to the incident or issue described in subparagraph (A); or

(C) any other entity or individual that the Board reasonably believes may have information relevant to the review and assessment carried out, or report issued, under subsection (e).

(2) VOLUNTARY PROVISION OF INFORMATION.—

(A) IN GENERAL.—Any entity or individual may voluntarily provide the Board with docu-

ments, including in electronic form, and testimony relevant to a review and assessment carried out, or report issued, by the Board under subsection (e), with or without a Board request for those documents or that testimony.

(B) BOARD REQUEST FOR INFORMATION.—If the Chair has reason to believe that an entity or individual has information relevant to an incident under review by the Board under subsection (e), the Chair, or an appropriate designee of the Chair, may request that information from the entity or individual.

(C) TREATMENT OF INFORMATION PROVIDED IN RESPONSE TO A BOARD REQUEST.—Any document, including in electronic form, or testimony provided to the Board in response to a request under subparagraph (B) shall be—

(i) treated as voluntarily provided; and

(ii) subject to the protections set forth under subsection (j).

(3) SUBPOENA AUTHORITY.—

(A) IN GENERAL.—If the Chair, or an appropriate designee of the Chair, determines that the response, or lack of a response, by an entity

or an individual to a request made under paragraph (2)(B) is deficient, the Chair, or an appropriate designee of the Chair, may, subject to approval under subparagraph (B)(i) of this paragraph, issue a subpoena to compel the disclosure of documents, including in electronic form, and testimony relevant to an incident under Board review under subsection (e).

(B) PROCEDURES.—

(i) IN GENERAL.—Before the issuance of a subpoena under subparagraph (A), a simple majority of the members of the Board must approve the issuance of the subpoena.

(ii) CONSIDERATIONS.—In evaluating whether to approve a subpoena under subparagraph (A), the members of the Board shall consider factors including—

(I) whether the Board is able to obtain the documents, including in electronic form, or testimony through other non-compulsory means;

(II) whether further communication with the entity or individual is likely to produce the documents, in-

cluding in electronic form, or testimony on a voluntary basis;

(III) whether, based on the nature of the request, a reasonable amount of time has elapsed to allow the entity or individual to voluntarily provide the documents, including in electronic form, or testimony to the Board;

(IV) the importance of the requested documents, including in electronic form, or testimony to the ability of the Board to complete a full and complete review and assessment or report under subsection (e); and

(V) whether, after consultation with relevant Federal agencies, the subpoena would affect a regulatory, law enforcement, foreign intelligence, or diplomatic effort of the United States.

(C) CIVIL ACTION.—

(i) IN GENERAL.—If an entity or individual fails to comply with a subpoena issued under this paragraph, the Chair

may refer the matter to the Attorney General to bring a civil action in an appropriate district court of the United States to enforce the subpoena.

(ii) VENUE.—An action under this subparagraph shall be brought in the judicial district in which the entity against which, or the individual against whom, the civil action is brought resides, is found, or does business, or in the District of Columbia.

(iii) CONTEMPT OF COURT.—A court may punish a failure to comply with a subpoena issued under this paragraph as contempt of court.

(D) EXCLUSION FOR GOVERNMENT ENTITIES.—This paragraph shall not apply to a State, local, Tribal, territorial, or Federal government entity, or to any employee of that entity with respect to matters related to the official duties of the employee.

(E) DELEGATION OF SUBPOENA AUTHORITY.—The authority of the Chair to issue a subpoena under this paragraph may only be delegated to another Board member.

(F) AUTHENTICATION.—

(i) IN GENERAL.—Any subpoena issued electronically under this paragraph shall be authenticated with a cryptographic digital signature, or other comparable successor technology, of the Chair or designee of the Chair, that allows the Chair or the designee of the Chair to demonstrate that the subpoena was issued by the Chair or the designee of the Chair and has not been altered or modified since the subpoena was issued.

(ii) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this paragraph that is not authenticated in accordance with clause (i) shall not be considered to be valid by the recipient of the subpoena or by any court.

(G) PRESERVATION.—For purposes of section 2703(f) of title 18, United States Code, the Board shall be considered to be a ''governmental entity''.

(H) PROTECTIONS FOR INFORMATION OBTAINED BY SUBPOENA.—Any document, includ-

ing in electronic form, or testimony obtained by a subpoena under this paragraph—

(i) shall not be subject to subsection (j); and

(ii) in the discretion of the Board, may be protected from public disclosure where otherwise consistent with applicable law.

(4) STORED COMMUNICATIONS ACT.—Nothing in this subsection 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'').

(5) INFORMATION FROM FEDERAL AGENCIES.—

(A) REQUESTS.—The Chair, or an appropriate designee of the Chair, may request from any Federal agency such information as necessary to carry out the duties of the Board.

(B) FURNISHING INFORMATION.—Upon request of the Chair, or the appropriate designee of the Chair, under subparagraph (A), the

head of a Federal agency shall furnish the applicable information to the Board.

(j) PROTECTIONS FOR INFORMATION VOLUNTARILY PROVIDED TO THE BOARD.—

(1) APPLICATION.—The protections in this subsection shall apply to any document, including in electronic form, or testimony voluntarily provided to the Board under subsection (i)(2).

(2) DISCLOSURE, RETENTION, AND USE.—Any document, including in electronic form, and testimony voluntarily provided to the Board may be disclosed to, retained by, and used by any Federal agency or department, component, officer, employee, or agent of the Federal Government, consistent with otherwise applicable provisions of Federal law, solely—

(A) for a cybersecurity purpose;

(B) to identify—

(i) a cybersecurity threat, including the source of the cybersecurity threat; or

(ii) a security vulnerability;

(C) to respond to, or otherwise prevent or mitigate, a specific threat of death, a specific threat of serious bodily harm, or a specific threat of serious economic harm, including a

terrorist act or use of a weapon of mass destruction;

(D) to respond to, investigate, prosecute, or otherwise prevent or mitigate, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(E) to prevent, investigate, disrupt, or prosecute an offense arising out of an incident or issue assessed by the Board, pursuant to subsection (e), or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015 (6 U.S.C. 1504(d)(5)(A)(v)).

(3) PROTECTIONS FOR ENTITIES AND INFORMATION.—Any document, including in electronic form, or testimony voluntarily provided to the Board under subsection (i)(2) shall—

(A) be considered the commercial, financial, and proprietary information of the providing entity or individual when so designated by that entity or individual;

(B) be exempt from disclosure under—

(i) section 552(b)(3) of title 5, United States Code (commonly known as the ''Freedom of Information Act''); and

(ii) any provision of State, Tribal, or local freedom of information law, open government law, open meetings law, open records law, sunshine law, or similar law requiring disclosure of information or records;

(C) be considered not to constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection; and

(D) not be subject to a rule of any Federal agency or any judicial doctrine regarding ex parte communications with a decision-making official.

(4) LIABILITY PROTECTIONS.—

(A) IN GENERAL.—No cause of action arising from the voluntary provision of documents to the Board under subsection (i)(2) shall lie or be maintained in any court by any person, and any such action shall be promptly dismissed.

(B) RESTRICTIONS.—

(i) IN GENERAL.—Subject to clause (ii), no submission voluntarily provided to the Board under subsection (i)(2), or any

communication, document, material, or other record, created for the sole purpose of preparing, drafting, or submitting such submission, may 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.

(ii) EXCEPTION.—This subparagraph shall not prevent the use, retention, or disclosure of information in the documents or testimony described in clause (i) to investigate or prosecute a person or entity suspected or alleged to have committed, conspired to commit, or aided and abetted the commission of, an incident described in the documents or testimony, provided that the submission itself is not disclosed.

(C) RULE OF CONSTRUCTION.—Nothing in this paragraph may be construed to create a defense to discovery or otherwise affect the discovery of any communication, document, material, or other record not created for the sole purpose of preparing, drafting, or submitting

such submission, except that this paragraph shall not apply to information developed from a source independent of a submission submitted under subsection (i)(2).

(k) ADDITIONAL PRIVACY AND DIGITAL SECURITY PROTECTIONS.—

(1) PRIVACY AND CIVIL LIBERTIES.—Any document, including in electronic form, or testimony provided to or obtained by the Board shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government in a manner that protects personal information from unauthorized use or unauthorized disclosure.

(2) DIGITAL SECURITY.—Any document, including in electronic form, or testimony provided to or obtained by the Board shall be collected, stored, and protected, at a minimum, in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199 of the National Institute of Standards and Technology, or any successor document.