Legislative Text:

A BILL

To establish the Cyber Safety Review Board, 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. CYBER SAFETY REVIEW BOARD.

(a) IN GENERAL.—Subtitle H of title VIII of the Homeland Security Act of 2002 (6 U.S.C. §§ 451 *et seq.*) is amended by adding at the end the following new sections:

"SEC. 890E. ESTABLISHMENT OF THE CYBER SAFETY REVIEW BOARD.

"(a) ESTABLISHMENT AND PURPOSE.—

"(1) The Secretary, in consultation with the Attorney General, shall establish the Cyber Safety Review Board (the Board) within the Department of Homeland Security.

"(2) The Board shall conduct independent and impartial reviews and assessments, with respect to cyber incidents affecting Federal civilian executive branch information systems or non-Federal information systems, threat activity, vulnerabilities, mitigation activities, and agency responses.

"(3) The Secretary shall ensure that the Board conducts independent, strategic, timely, specific and actionable reviews and assessments.

"(b) CONVENING THE BOARD.—The Chair, designated by the Secretary pursuant to subsection (d)(3), shall convene the Board—

"(1) at any time as directed by the President;

"(2) at any time the Secretary deems necessary, including following a "significant cyber incident," as defined by section 2240(9) of this Act, or upon the declaration of a "significant incident" in accordance with section 2233(a) of this Act; or

"(3) upon a two-thirds majority vote of the Board.

"(c) REPORTS CONTAINING ADVICE AND RECOMMENDATIONS.—

"(1) After the Board convenes pursuant to subsection (b), the Board shall conduct a review and assessment of the incident or issue for which it was convened. Following completion of the review and assessment, the Board shall prepare a report, to include findings, advice, and recommendations for improving cybersecurity and incident

response practices and policy, and upon completion of this report, the Chair shall transmit it to the Secretary.

"(2) Upon review of the report, the Secretary shall, consistent with the protections for documents (including in electronic form) and testimony voluntarily provided to the Board under section 890G, share the report (or portions thereof) with interested or affected parties, including the general public.

"(3) No report or portion of a report of the Board may be admitted into evidence in a civil action for damages resulting from a matter mentioned in the report.

"(d) MEMBERSHIP.—

"(1) IN GENERAL.—The Board shall consist of no more than 20 standing members appointed by the Secretary, with the number of Federal members or non-Federal members never exceeding each other by more than one member.

"(A) FEDERAL MEMBERSHIP.—Federal membership of the Board shall include, at least, one appointed representative from each of the following:

"(i) the Department;

"(ii) the Cybersecurity and Infrastructure Security Agency;

"(iii) the Department of Defense;

"(iv) the National Security Agency;

"(v) the Department of Justice;

"(vi) the Federal Bureau of Investigation; and

"(vii) the Office of the National Cyber Director.

"(B) NON-FEDERAL MEMBERSHIP.—

"(i) As appropriate, the Secretary shall appoint to the Board non-Federal members, who may include individuals from nonprofit organizations, academia, private cybersecurity providers, software suppliers, critical infrastructure operators, or other experts in cybersecurity. Non-Federal members shall serve for terms of two years (renewable up to two years).

"(ii) ROLE OF NON-FEDERAL MEMBERS.—Non-Federal members appointed to the Board shall operate in their personal capacity and shall

provide their independent expertise to the Board, rather than represent the views of any current or previous employer.

"(iii) STATUS OF NON-FEDERAL MEMBERS.—A non-Federal member shall not be considered an employee of the Federal Government by reason of any service on the Board, except for the purposes of the following provisions of law:

"(I) section 5703 of title 5, United States Code, relating to travel expenses;

"(II) chapter 81 of title 5, United States Code, relating to compensation for work-related injuries;

"(III) chapter 171 of title 28, United States Code, and any other Federal statute relating to tort liability;

"(IV) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18, United States Code; and

"(V) the Ethics in Government Act of 1978;

"(iv) PAY.—A non-Federal member of the Board may not receive pay by reason of service on the Board.

"(v) REQUIREMENTS.—As required or permitted by law, non-Federal members appointed to the Board shall—

"(I) complete all required financial disclosure forms and ethics training;

"(II) may not participate personally and substantially in any particular matter, including any investigation, request for information, cyber incident review or assessment, in which the member's non-Federal employer has a financial interest;

"(III) obtain and maintain a security clearance; and

"(IV) sign and adhere to non-disclosure agreements pertaining to the work of the Board.

"(2) ADDITIONAL PARTICIPATION.—

"(A) When the Board reviews an incident that involves Federal civilian executive branch information systems, as determined by the Secretary, the

Secretary shall invite a representative from the Office of Management and Budget to participate in Board activities.

"(B) As appropriate, and on a case-by-case basis depending on the nature of the incident under review, the Secretary may invite additional individuals to participate in the work of the Board on a temporary basis.

"(3) BOARD CHAIR AND DEPUTY CHAIR.—Every two years, the Secretary shall designate a Chair and Deputy Chair of the Board from among the members of the Board. The Secretary shall designate the Chair from among the Federal members of the Board, and the Secretary shall designate the Deputy Chair from the non-Federal members. If the Chair or Deputy Chair departs the Board prior to the expiration of the Chair's or Deputy Chair's term, the Secretary shall designate a new Chair or Deputy Chair consistent with this subsection.

"(e) PERSONNEL.—In order to support the work of the Board, the Secretary shall assign permanent staff to the Board and may detail Department and other Federal department or agency personnel to support the Board. The detail of Department or other Federal department or agency personnel under this subsection may be on a reimbursable or non-reimbursable basis.

"(f) PROTECTION OF INFORMATION.—The Secretary and the Board shall protect sensitive law enforcement, operational, business, and other confidential documents (including in electronic form) and testimony voluntarily provided to the Board consistent with section 890G.

"(g) EXEMPTION FROM APPLICABLE LAW.—The Board established by the Secretary pursuant to subsection (a) of this section shall be exempt from—

"(1) Chapter 10 of title 5, United States Code (commonly known as the Federal Advisory Committee Act); and

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

"(h) BOARD MANAGEMENT.—

"(1) To ensure that the Board fulfills its purpose as described in subsection (a), the Chair designated under subsection (d)(3) shall take all necessary actions to manage the affairs of the Board and the conduct of Board reviews and assessments. Such actions shall include--

"(A) developing and promulgating, with the approval of the Board, bylaws and internal procedures concerning the work of the Board; and

"(B) making contracts and entering into agreements with other Federal departments and agencies as necessary and appropriate to carry out the Board's responsibilities.

"(2) The Secretary shall implement a system to identify, mitigate, and manage any conflicts of interest that may arise as a result of an individual's participation in the work of the Board under this section.

"SEC. 890F. REQUESTS FOR INFORMATION AND ADMINISTRATIVE SUBPOENAS.

"(a) PURPOSE.—In order to ensure that the Board established under subsection 890E(a) has sufficient information to conduct its required reviews and assessments and issue reports to the Secretary, the Chair designated pursuant to subsection 890E(c)(3), or an appropriate designee, may request and receive relevant documents (including in electronic form) and testimony from and issue subpoenas to (i) entities or individuals affected by the incident or issue giving rise to the review and assessment, (ii) entities that, or individuals who, responded to the incident or issue, or (iii) any other entity or individual that the Board reasonably believes may have information relevant to the review and assessment or report.

"(b) VOLUNTARY PROVISION OF INFORMATION.—

"(1) IN GENERAL.—Entities and individuals may voluntarily provide the Board with documents (including in electronic form) and testimony relevant to a Board's review and assessment and/or report with or without a Board request.

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

"(3) TREATMENT OF INFORMATION PROVIDED IN RESPONSE TO A BOARD REQUEST.—Documents (including in electronic form) and testimony provided to the Board in response to a request under paragraph (2) shall be treated as voluntarily provided and thus subject to the protections set forth under section 890G.

"(c) SUBPOENA.—

"(1) IN GENERAL.—If the Chair or appropriate designee deems an entity's or individual's response, or lack thereof, to a request made pursuant to subsection (b)(2) to be deficient for any reason, the Chair may issue to the entity or individual a subpoena to compel the disclosure of documents (including in electronic form) and testimony relevant a cybersecurity incident under Board review in accordance with the procedures described in subsection (c)(2)(A).

"(2) PROCEDURES.—

"(A) BOARD APPROVAL.—Prior to the Chair's issuance of a subpoena under this subsection, a two-thirds majority of a quorum of the Board members casting votes (excluding the members described in subsection (c)(2)(B)) must approve the issuance of a subpoena to an entity or individual. In evaluating whether to approve a subpoena under this subsection, the Board shall, in its sole discretion, take into consideration factors including—

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

"(ii) whether further communication with the entity or individual is likely to produce documents (including in electronic form) and 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) and testimony to the Board;

"(iv) the importance of the requested documents (including in electronic form) and testimony to the Board's ability to complete a full and complete review and assessment or report; and

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

"(B) NON-FEDERAL BOARD MEMBERS EXCLUDED.—Non-Federal members of the Board shall be excluded from deliberations and voting on the issuance of a subpoena pursuant to this subsection. While non-Federal members

may make a recommendation to the Board, to include presenting information in support of the recommendation, that a subpoena be issued as necessary for a Board assessment or report, non-Federal members shall be excluded from any subsequent deliberations and voting on the recommendation.

"(3) CIVIL ACTION.—

"(A) IN GENERAL.—If an entity or individual fails to comply with a subpoena issued pursuant to this subsection, the Chair may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce the subpoena.

"(B) VENUE.—An action under this subsection may 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.

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

"(4) EXCLUSION FOR GOVERNMENT ENTITIES.—This subsection shall not apply to a State, local, Tribal, territorial, or Federal government entity, or to employees of that entity with respect to matters related to their official duties.

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

"(6) AUTHENTICATION.—

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

"(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued electronically pursuant to this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of the subpoena or by any court.

"(7) PRESERVATION.—The Board shall be a "governmental entity" for purposes of 18 U.S.C. 2703(f).

"(8) PROTECTIONS FOR INFORMATION OBTAINED BY SUBPOENA.—Documents (including in electronic form) and testimony obtained by a subpoena under this subsection shall not be subject to Section 890G but, in the discretion of the Board, may be protected from public disclosure where otherwise consistent with applicable law.

"(d) STORED COMMUNICATIONS ACT.—Nothing in this section shall 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. 890G. PROTECTIONS FOR INFORMATION VOLUNTARILY PROVIDED TO THE BOARD.

"(a) IN GENERAL.—The protections in this section shall apply to documents (including in electronic form) and testimony voluntarily provided to the Board pursuant to subsection 890F(b).

"(b) DISCLOSURE, RETENTION, AND USE.—Documents (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 —

"(1) for a cybersecurity purpose;

"(2) to identify—

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

"(B) a security vulnerability;

"(3) 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;

"(4) 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

"(5) to prevent, investigate, disrupt, or prosecute an offense arising out of an incident or issue assessed by the Board or any of the offenses listed in

section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015, Div. N of Pub. L. No. 114-113, the Consolidated Appropriations Act, 2016 (6 U.S.C. 1504(d)(5)(A)(v)).

"(c) PROTECTIONS FOR ENTITIES AND INFORMATION.—Documents (including in electronic form) and testimony voluntarily provided to the Board shall—

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

"(2) be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the "Freedom of Information Act"), as well as 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;

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

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

"(d) LIABILITY PROTECTIONS.—

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

"(2) RESTRICTIONS.—No submission voluntarily provided to the Board 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 thereof, provided that (A) this paragraph shall not prevent the use, retention, or disclosure of information in the documents or testimony to investigate or prosecute a person or entity suspected or alleged to have committed, conspired to commit, or aided and abetted the commission of, a cyber incident described in the documents or testimony as long as the submission itself is not disclosed and (B) nothing in this part shall 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. This paragraph does not apply to information developed from a source independent of a submission under subsection 890F(b).

"(e) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—

"(1) IN GENERAL.—A Federal, State, local, Tribal, or territorial government shall not use information obtained solely through the voluntarily provision of documents (including in electronic form) and testimony to the Board to regulate or take an enforcement action against the activities of the entity that, or individual who, voluntarily provided the information.

"(2) CLARIFICATION.—Documents (including in electronic form) and testimony voluntarily provided to the Board may, consistent with Federal or State regulatory authority relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to those systems.

"SEC. 890H. ADDITIONAL PRIVACY AND DIGITAL SECURITY PROTECTIONS.

"(a) PRIVACY AND CIVIL LIBERTIES.—Documents (including in electronic form) and 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.

"(b) DIGITAL SECURITY.—Documents (including in electronic form) and 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, or any successor document.

"SEC. 890I. DEFINITIONS.

"For the purposes of sections 890E through 890H—

"(1) the term 'Federal civilian executive branch information systems' means information systems operated by Federal civilian executive branch agencies, with the exception of information systems as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3);

"(2) the term 'Federal civilian executive branch agencies' means all Federal agencies except for the Department of Defense and agencies in the Intelligence Community;

"(3) the term 'incident' has the meaning given the term in section 2200(12) of this Act;

"(4) the term 'information system' has the meaning given the term in section 2200(14) of this Act;

"(5) the terms 'cybersecurity purpose,' 'cybersecurity threat,' and 'security vulnerability' have the meanings given those terms in section 2200 of this Act.".

(b) CLERICAL AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (6 U.S.C. 101 note) is amended by inserting after the item relating to section 890D the following new items:

SEC. 2. CONFORMING AMENDMENTS.

The Homeland Security Act of 2002 is amended—

(1) in the table of contents in section 1(b) (6 U.S.C. 101 note), by amending the item relating to section 2245 by striking "Information" and inserting by "Protections for information"; and

(2) in section 2245 (6 U.S.C. 681e)—

(A) in the section heading, by inserting "**PROTECTIONS FOR**" before "**INFORMATION**"; and

(B) in subsection (c)(2), by striking "litigation" and inserting "a cause of action".

A Bill to Establish the Cyber Safety Review Board

Comparative type:

HOMELAND SECURITY ACT OF 2002

* * * * * * *

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) * * * * * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle H—Miscellaneous Provisions

* * * * * * *

Sec. 890D. Mentor-Protégé Program.
Sec. 890E. Establishment of the Cyber Safety Review Board.
Sec. 890F. Requests for Information and Administrative Subpoenas.
Sec. 890G. Protections for Information Voluntarily Provided to the Board.
Sec. 890H. Additional Privacy and Data Security Protections.
Sec. 890I. Definitions.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle D—Cyber Incident Reporting

* * * * * * *

Sec. 2245. **[Information]** **Protections for information** shared with or provided to the Federal Government.

* * * * * * *

TITLE VIII—COORDINATION WITH NON-FEDERAL ENTITIES; INSPECTOR GENERAL; UNITED STATES SECRET SERVICE; COAST GUARD; GENERAL PROVISIONS

* * * * * * *

Subtitle H—Miscellaneous Provisions

* * * * * * *

SEC. 890E. ESTABLISHMENT OF THE CYBER SAFETY REVIEW BOARD.

(a) ESTABLISHMENT AND PURPOSE.—

(1) The Secretary, in consultation with the Attorney General, shall establish the Cyber Safety Review Board (the Board) within the Department of Homeland Security.

(2) The Board shall conduct independent and impartial reviews and assessments, with respect to cyber incidents affecting Federal civilian executive branch information systems or non-Federal information systems, threat activity, vulnerabilities, mitigation activities, and agency responses.

(3) The Secretary shall ensure that the Board conducts independent, strategic, timely, specific and actionable reviews and assessments.

(b) CONVENING THE BOARD.—The Chair, designated by the Secretary pursuant to subsection (d)(3), shall convene the Board—

(1) at any time as directed by the President;

(2) at any time the Secretary deems necessary, including following a "significant cyber incident," as defined by section 2240(9) of this Act, or upon the declaration of a "significant incident" in accordance with section 2233(a) of this Act; or

(3) upon a two-thirds majority vote of the Board.

(c) REPORTS CONTAINING ADVICE AND RECOMMENDATIONS.—

(1) After the Board convenes pursuant to subsection (b), the Board shall conduct a review and assessment of the incident or issue for which it was convened. Following completion of the review and assessment, the Board shall prepare a report, to include findings, advice, and recommendations for improving cybersecurity and incident response practices and policy, and upon completion of this report, the Chair shall transmit it to the Secretary.

(2) Upon review of the report, the Secretary shall, consistent with the protections for documents (including in electronic form) and testimony voluntarily provided to the Board under section 890G, share the report (or portions thereof) with interested or affected parties, including the general public.

(3) No report or portion of a report of the Board may be admitted into evidence in a civil action for damages resulting from a matter mentioned in the report.

(d) MEMBERSHIP.—

(1) IN GENERAL.—The Board shall consist of no more than 20 standing members appointed by the Secretary, with the number of Federal members or non-Federal members never exceeding each other by more than one member.

(A) FEDERAL MEMBERSHIP.—Federal membership of the Board shall include, at least, one appointed representative from each of the following:

(i) the Department;
(ii) the Cybersecurity and Infrastructure Security Agency;
(iii) the Department of Defense;
(iv) the National Security Agency;
(v) the Department of Justice;
(vi) the Federal Bureau of Investigation; and
(vii) the Office of the National Cyber Director.

(B) NON-FEDERAL MEMBERSHIP.—

(i) As appropriate, the Secretary shall appoint to the Board non-Federal members, who may include individuals from nonprofit organizations, academia, private cybersecurity providers, software suppliers, critical infrastructure operators, or other experts in cybersecurity. Non-Federal members shall serve for terms of two years (renewable up to two years).

(ii) ROLE OF NON-FEDERAL MEMBERS.—Non-Federal members appointed to the Board shall operate in their personal capacity and shall provide their independent expertise to the Board, rather than represent the views of any current or previous employer.

(iii) STATUS OF NON-FEDERAL MEMBERS.—A non-Federal member shall not be considered an employee of the Federal Government by reason of any service on the Board, except for the purposes of the following provisions of law:

(I) section 5703 of title 5, United States Code, relating to travel expenses;

(II) chapter 81 of title 5, United States Code, relating to compensation for work-related injuries;

(III) chapter 171 of title 28, United States Code, and any other Federal statute relating to tort liability;

(IV) sections 201, 203, 205, 207, 208, 209, 603, 606, 607, 643, 654, 1905, and 1913 of title 18, United States Code; and

(V) the Ethics in Government Act of 1978;

(iv) PAY.—A non-Federal member of the Board may not receive pay by reason of service on the Board.

(v) REQUIREMENTS.—As required or permitted by law, non-Federal members appointed to the Board shall—

(I) complete all required financial disclosure forms and ethics training;

(II) may not participate personally and substantially in any particular matter, including any investigation, request for information, cyber incident review or assessment, in which the member's non-Federal employer has a financial interest;

(III) obtain and maintain a security clearance; and

(IV) sign and adhere to non-disclosure agreements pertaining to the work of the Board.

(2) ADDITIONAL PARTICIPATION.—

(A) When the Board reviews an incident that involves Federal civilian executive branch information systems, as determined by the Secretary, the Secretary shall invite a representative from the Office of Management and Budget to participate in Board activities.

(B) As appropriate, and on a case-by-case basis depending on the nature of the incident under review, the Secretary may invite additional individuals to participate in the work of the Board on a temporary basis.

(3) BOARD CHAIR AND DEPUTY CHAIR.—Every two years, the Secretary shall designate a Chair and Deputy Chair of the Board from among the members of the Board. The Secretary shall designate the Chair from among the Federal members of the Board, and the Secretary shall designate the Deputy Chair from the non-Federal members. If the Chair or Deputy Chair departs the Board prior to the expiration of the Chair's or Deputy Chair's term, the Secretary shall designate a new Chair or Deputy Chair consistent with this subsection.

(e) PERSONNEL.—In order to support the work of the Board, the Secretary shall assign permanent staff to the Board and may detail Department and other Federal department or agency personnel to support the Board. The detail of Department or other Federal department or agency personnel under this subsection may be on a reimbursable or non-reimbursable basis.

(f) PROTECTION OF INFORMATION.—The Secretary and the Board shall protect sensitive law enforcement, operational, business, and other confidential documents (including in electronic form) and testimony voluntarily provided to the Board consistent with section 890G.

(g) EXEMPTION FROM APPLICABLE LAW.—The Board established by the Secretary pursuant to subsection (a) of this section shall be exempt from—

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

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

(h) BOARD MANAGEMENT.—

(1) To ensure that the Board fulfills its purpose as described in subsection (a), the Chair designated under subsection (d)(3) shall take all necessary actions to manage the affairs of the Board and the conduct of Board reviews and assessments. Such actions shall include--

(A) developing and promulgating, with the approval of the Board, bylaws and internal procedures concerning the work of the Board; and

(B) making contracts and entering into agreements with other Federal departments and agencies as necessary and appropriate to carry out the Board's responsibilities.

(2) The Secretary shall implement a system to identify, mitigate, and manage any conflicts of interest that may arise as a result of an individual's participation in the work of the Board under this section.

SEC. 890F. REQUESTS FOR INFORMATION AND ADMINISTRATIVE SUBPOENAS.

(a) PURPOSE.—In order to ensure that the Board established under subsection 890E(a) has sufficient information to conduct its required reviews and assessments and issue reports to the Secretary, the Chair designated pursuant to subsection 890E(c)(3), or an appropriate designee, may request and receive relevant documents (including in electronic form) and testimony from and issue subpoenas to (i) entities or individuals affected by the incident or issue giving rise to the review and assessment, (ii) entities that, or individuals who, responded to the incident or issue, or (iii) any other entity or individual that the Board reasonably believes may have information relevant to the review and assessment or report.

(b) VOLUNTARY PROVISION OF INFORMATION.—

(1) IN GENERAL.—Entities and individuals may voluntarily provide the Board with documents (including in electronic form) and testimony relevant to a Board's review and assessment and/or report with or without a Board request.

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

(3) TREATMENT OF INFORMATION PROVIDED IN RESPONSE TO A BOARD REQUEST.—Documents (including in electronic form) and testimony provided to the Board in response to a request under paragraph (2) shall be treated as voluntarily provided and thus subject to the protections set forth under section 890G.

(c) SUBPOENA.—

(1) IN GENERAL.—If the Chair or appropriate designee deems an entity's or individual's response, or lack thereof, to a request made pursuant to subsection (b)(2) to be deficient for any reason, the Chair may issue to the entity or individual a subpoena to compel the disclosure of documents (including in electronic form) and testimony relevant a cybersecurity incident under Board review in accordance with the procedures described in subsection (c)(2)(A).

(2) PROCEDURES.—

(A) BOARD APPROVAL.—Prior to the Chair's issuance of a subpoena under this subsection, a two-thirds majority of a quorum of the Board members casting votes (excluding the members described in subsection (c)(2)(B)) must approve the issuance of a subpoena to an entity or individual. In evaluating whether to approve a subpoena under this subsection, the Board shall, in its sole discretion, take into consideration factors including—

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

(ii) whether further communication with the entity or individual is likely to produce documents (including in electronic form) and 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) and testimony to the Board;

(iv) the importance of the requested documents (including in electronic form) and testimony to the Board's ability to complete a full and complete review and assessment or report; and

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

(B) NON-FEDERAL BOARD MEMBERS EXCLUDED.—Non-Federal members of the Board shall be excluded from deliberations and voting on the issuance of a subpoena pursuant to this subsection. While non-Federal members may make a recommendation to the Board, to include presenting information in support of the recommendation, that a subpoena be issued as

necessary for a Board assessment or report, non-Federal members shall be excluded from any subsequent deliberations and voting on the recommendation.

(3) CIVIL ACTION.—

(A) IN GENERAL.—If an entity or individual fails to comply with a subpoena issued pursuant to this subsection, the Chair may refer the matter to the Attorney General to bring a civil action in a district court of the United States to enforce the subpoena.

(B) VENUE.—An action under this subsection may 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.

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

(4) EXCLUSION FOR GOVERNMENT ENTITIES.—This subsection shall not apply to a State, local, Tribal, territorial, or Federal government entity, or to employees of that entity with respect to matters related to their official duties.

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

(6) AUTHENTICATION.—

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

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

(7) PRESERVATION.—The Board shall be a "governmental entity" for purposes of 18 U.S.C. 2703(f).

(8) PROTECTIONS FOR INFORMATION OBTAINED BY SUBPOENA.—Documents (including in electronic form) and testimony obtained by a subpoena under this subsection shall not be subject to Section 890G but, in the discretion of the Board, may be protected from public disclosure where otherwise consistent with applicable law.

(d) STORED COMMUNICATIONS ACT.—Nothing in this section shall 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. 890G. PROTECTIONS FOR INFORMATION VOLUNTARILY PROVIDED TO THE BOARD.

(a) IN GENERAL.—The protections in this section shall apply to documents (including in electronic form) and testimony voluntarily provided to the Board pursuant to subsection 890F(b).

(b) DISCLOSURE, RETENTION, AND USE.—Documents (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—

(1) for a cybersecurity purpose;

(2) to identify—

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

(B) a security vulnerability;

(3) 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;

(4) 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

(5) to prevent, investigate, disrupt, or prosecute an offense arising out of an incident or issue assessed by the Board or any of the offenses listed in section 105(d)(5)(A)(v) of the Cybersecurity Act of 2015, Div. N of Pub. L. No. 114-113, the Consolidated Appropriations Act, 2016 (6 U.S.C. 1504(d)(5)(A)(v)).

(c) PROTECTIONS FOR ENTITIES AND INFORMATION.—Documents (including in electronic form) and testimony voluntarily provided to the Board shall—

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

(2) be exempt from disclosure under section 552(b)(3) of title 5, United States Code (commonly known as the "Freedom of Information Act"), as well as 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;

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

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

(d) LIABILITY PROTECTIONS.—

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

(2) RESTRICTIONS.—No submission voluntarily provided to the Board 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 thereof, provided that (A) this paragraph shall not

prevent the use, retention, or disclosure of information in the documents or testimony to investigate or prosecute a person or entity suspected or alleged to have committed, conspired to commit, or aided and abetted the commission of, a cyber incident described in the documents or testimony as long as the submission itself is not disclosed and (B) nothing in this part shall 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. This paragraph does not apply to information developed from a source independent of a submission under subsection 890F(b).

(e) PROHIBITION ON USE OF INFORMATION IN REGULATORY ACTIONS.—

(1) IN GENERAL.—A Federal, State, local, Tribal, or territorial government shall not use information obtained solely through the voluntarily provision of documents (including in electronic form) and testimony to the Board to regulate or take an enforcement action against the activities of the entity that, or individual who, voluntarily provided the information.

(2) CLARIFICATION.—Documents (including in electronic form) and testimony voluntarily provided to the Board may, consistent with Federal or State regulatory authority relating to the prevention and mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to those systems.

SEC. 890H. ADDITIONAL PRIVACY AND DIGITAL SECURITY PROTECTIONS.

(a) PRIVACY AND CIVIL LIBERTIES.—Documents (including in electronic form) and 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.

(b) DIGITAL SECURITY.—Documents (including in electronic form) and 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, or any successor document.

SEC. 890I. DEFINITIONS.

For the purposes of sections 890E through 890H—

(1) the term "Federal civilian executive branch information systems" means information systems operated by Federal civilian executive branch agencies, with the exception of information systems as defined in 44 U.S.C. 3552(b)(6), 3553(e)(2), and 3553(e)(3);

(2) the term "Federal civilian executive branch agencies" means all Federal agencies except for the Department of Defense and agencies in the Intelligence Community;

(3) the term "incident" has the meaning given the term in section 2200(12) of this Act;

(4) the term "information system" has the meaning given the term in section 2200(14) of this Act;

(5) the terms "cybersecurity purpose," "cybersecurity threat," and "security vulnerability" have the meanings given those terms in section 2200 of this Act.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

* * * * * * *

Subtitle D—Cyber Incident Reporting

* * * * * * *

SEC. 2245. **[INFORMATION]** **PROTECTIONS FOR INFORMATION** SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.

(a) * * * * * * *

(b) * * * * * * *

(c) LIABILITY PROTECTIONS.—

(1) * * * * * * *

(2) SCOPE.—The liability protections provided in this subsection shall only apply to or affect **[litigation]** **a cause of action** that is solely based on the submission of a covered cyber incident report or ransom payment report to the Agency.

(3) * * * * * * *

* * * * * * *

Analysis:

Originally established by the Secretary of Homeland Security pursuant to Executive Order No. 14028, *Improving the Nation's Cybersecurity,* the Cyber Safety Review Board (CSRB) reviews and assesses threat activity, vulnerabilities, mitigation activities, and agency responses related to "significant cyber incidents" affecting federal civilian executive branch information systems and non-federal systems.[1] As set forth in Executive Order No. 14028, the CSRB consists of both federal members (including representatives of the Department of Defense, the Department of Justice, the Cybersecurity and Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigation) and non-federal members who serve as Special Government Employees for the duration of their appointment to the Board.[2] Since its inception, the CSRB has published its initial "Review of the December 2021

[1] Exec. Order No. 14028 § 5(b) (May 12, 2021); *see also* Presidential Policy Directive 41 (July 26, 2016) (defining a "significant cyber incident" as "[a] cyber incident that is (or group of related cyber incidents that together are) 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 American people").

[2] *See* 18 U.S.C. § 202(a).

log4j Event" in July 2022[3] and has recently, as required by Section 5(i) of Executive Order No. 14028, prepared a second report (the "Section 5(i) Report") for the President on a series of issues:

- gaps in, and options for, the Board's composition or authorities;
- the Board's proposed mission, scope, and responsibilities;
- membership eligibility criteria for private-sector representatives;
- the Board's governance structure, including interaction with the executive branch and the Executive Office of the President;
- thresholds and criteria for the types of cyber incidents to be evaluated;
- sources of information that should be made available to the Board, consistent with applicable law and policy;
- an approach for protecting the information provided to the Board and securing the cooperation of affected United States individuals and entities for the purpose of the Board's review of incidents; and
- administrative and budgetary considerations required for operation of the Board.

In considering the above issues and preparing the Section 5(i) Report, the CSRB developed a legislative proposal to, among other things, codify the CSRB in statute and provide it with additional authorities that respond to identified gaps and will better support future reviews and assessments. The proposed legislative text contains four primary sections,[4] which, if enacted, would be codified as part of Subtitle H of Title VIII of the Homeland Security Act of 2002.

The first section (proposed Section 890E of the Homeland Security Act of 2002) is largely based on the CSRB structure as set forth in Executive Order No. 14028 and the CSRB Charter; it directs the Secretary of Homeland Security to establish the CSRB within the Department of Homeland Security, sets forth the CSRB's purpose, and specifies the conditions for convening the Board.[5] This section also directs the CSRB to provide the results of its reviews and assessments, to include findings, advice, and recommendations for improving cybersecurity and incident response practices and policy, directly to the Secretary of Homeland Security, who shall make the CSRB report, or portions of thereof, public, consistent with information protections set forth in the third section of the proposal, discussed below. Additionally, this section establishes that the CSRB includes both federal and non-federal members; provides for additional CSRB participation in certain circumstances; exempts the

[3] https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.

[4] In addition to the four substantive sections, the proposal also makes minor technical corrections to section 2245 of the Homeland Security Act of 2002 (the Act), 6 U.S.C. § 681e, and contains a section with definitions of key terms in the proposal.

[5] The proposal mandates that the Board convene as directed by the President, as deemed necessary by the Secretary of Homeland Security (including following a "significant cyber incident," as defined by section 2240(9) of the Act, 6 U.S.C. § 681(9), or upon the declaration of a "significant incident" in accordance with section 2233(a) of the Act, 6 U.S.C. § 677b(a)), or upon a two-thirds majority vote of the Board.

CSRB from the Federal Advisory Committee Act[6] and the Government in the Sunshine Act; and establishes the CSRB Chair and Deputy Chair. This section directs the Chair to take all necessary actions, including developing and promulgating bylaws and internal procedures, to manage the CSRB consistent with its statutory purpose and directs the Secretary of Homeland Security to implement a system to identify, mitigate, and manage any conflicts of interest that may arise as a result of an individual's participation in the work of the Board.

The second section (proposed Section 890F of the Homeland Security Act of 2002), adapted from a provision in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"),[7] establishes the mechanisms by which the CSRB obtains the information needed to conduct its reviews and assessments. This section provides that the Chair or designee may request documents and testimony from relevant entities or individuals and that documents and testimony voluntarily provided, whether prior to or after a Chair request, receive the protections set forth in the third section of the proposal, discussed below. This section further provides that if the Chair receives no response or an inadequate or incomplete response to a request, the Chair may, with Board approval, issue a subpoena to compel disclosure of the requested documents and testimony. This provision sets out discretionary factors for the Board's consideration prior to issuance of a subpoena, including whether the Board is able to obtain the documents and testimony though other, non-compulsory means; whether a reasonable amount of time has passed to allow for voluntary provision of the documents and testimony; whether further communication would likely yield a voluntary response; and the importance of the documents and testimony to the review or assessment. Given the mixed federal and non-federal composition of the CSRB's membership, this section specifically excludes non-federal members from deliberations and voting on any subpoena.[8] This section also authorizes the Chair to make referrals to the Attorney General to enforce compliance with an issued subpoena.

The third section (proposed Section 890G of the Homeland Security Act of 2002), also based on a provision in CIRCIA,[9] imposes a number of limitations on the federal government's retention, disclosure, and use of documents and testimony voluntarily provided to the CSRB. This section also provides a number of additional protections to voluntarily provided documents and testimony, such as exemption from disclosure under the Freedom of Information Act[10] and similar state, local, or Tribal open government or disclosure laws. Further, this section provides liability protections to preclude any cause of action arising from the voluntary provision of documents and testimony to the Board, and it protects entities and individuals from enforcement

---

[6] Note that, consistent with section 871(a) of the Homeland Security Act of 2002, 6 U.S.C. § 451(a), the Secretary of Homeland Security already exempted the CSRB from the Federal Advisory Committee Act. 87 Fed. Reg. 6195, 6195 (Feb. 3, 2022).

[7] *See generally* Homeland Security Act of 2002 § 2244, 6 U.S.C. § 681d.

[8] As set forth in the proposal, however, non-federal CSRB members may recommend issuance of a subpoena and provide information in support of such a recommendation.

[9] *See generally* Homeland Security Act of 2002 § 2245, 6 U.S.C. § 681e.

[10] 5 U.S.C. § 552(b)(3).

or regulatory action based solely on documents and testimony voluntarily provided to the Board.[11]

The fourth section (proposed Section 890H of the Homeland Security Act of 2002), also adapted from relevant language in CIRCIA,[12] states that documents and testimony provided to or obtained by the CSRB are subject to privacy and civil liberties protections for personal information and requires that, at minimum, the CSRB employ digital security protections in accordance with the requirements applicable to the collection, storing, and protecting of information for moderate impact federal information systems.

[11] However, consistent with applicable federal or state authority related to the prevention or mitigation of cybersecurity threats to information systems, the information provided may be used to inform the development or implementation of regulations relating to such systems.

[12] *See* Homeland Security Act of 2002 § 2245(a)(3), (a)(4), 6 U.S.C. § 681e(a)(3), (a)(4).