AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.

S. 2540

To make technical corrections to title XXII of the Homeland Security Act of 2002, and for other purposes.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. PORTMAN (for himself and Mr. PETERS)

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''CISA Technical Corrections and Improvements Act of 2021''.

SEC. 2. REDESIGNATIONS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(1) by redesignating section 2217 (6 U.S.C. 665f) as section 2220;

(2) by redesignating section 2216 (6 U.S.C. 665e) as section 2219;

(3) by redesignating the fourth section 2215 (relating to Sector Risk Management Agencies) (6 U.S.C. 665d) as section 2218;

(4) by redesignating the third section 2215 (relating to the Cybersecurity State Coordinator) (6 U.S.C. 665c) as section 2217; and

(5) by redesignating the second section 2215 (relating to the Joint Cyber Planning Office) (6 U.S.C. 665b) as section 2216.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 2202(c) of the Homeland Security Act of 2002 (6 U.S.C. 652(c)) is amended—

(1) in the first paragraph (12), by striking ''section 2215'' and inserting ''section 2217''; and

(2) by redesignating the second and third paragraphs (12) as paragraphs (13) and (14), respectively.

(c) ADDITIONAL TECHNICAL AMENDMENT.—

(1) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland

Security Act'' and inserting ''Homeland Security Act of 2002''.

(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall take effect as if enacted as part of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260).

SEC. 3. CONSOLIDATION OF DEFINITIONS.

(a) IN GENERAL.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651) is amended by inserting before the subtitle A heading the following:

''SEC. 2200. DEFINITIONS.

''Except as otherwise specifically provided, in this title:

''(1) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(2) AGENCY INFORMATION.—The term 'agency information' means information collected or maintained by or on behalf of an agency.

''(3) AGENCY INFORMATION SYSTEM.—The term 'agency information system' means an information system used or operated by an agency or by another entity on behalf of an agency.

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

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

"(B) the Committee on Homeland Security of the House of Representatives.

"(5) CRITICAL INFRASTRUCTURE INFORMATION.—The term 'critical infrastructure information' means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

"(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

"(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including secu-

rity testing, risk evaluation thereto, risk management planning, or risk audit; or

''(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

''(6) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' means information that is necessary to describe or identify—

''(A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;

''(B) a method of defeating a security control or exploitation of a security vulnerability;

''(C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;

''(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly

enable the defeat of a security control or exploitation of a security vulnerability;

''(E) malicious cyber command and control;

''(F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;

''(G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or

''(H) any combination thereof.

''(7) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' means the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.

''(8) CYBERSECURITY RISK.—The term 'cybersecurity risk'—

''(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruc-

tion of such information or information systems, including such related consequences caused by an act of terrorism; and

"(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

"(9) CYBERSECURITY THREAT.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'cybersecurity threat' means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system.

"(B) EXCLUSION.—The term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement.

"(10) DEFENSIVE MEASURE.—

"(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'defensive measure'

means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

''(B) EXCLUSION.—The term 'defensive measure' does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

''(i) the entity operating the measure; or

''(ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

''(11) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and tribal government officials, private

sector representatives, academics, and other policy experts.

"(12) INCIDENT.—The term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

"(13) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'Information Sharing and Analysis Organization' means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of—

"(A) gathering and analyzing critical infrastructure information, including information related to cybersecurity risks and incidents, in order to better understand security problems and interdependencies related to critical infrastructure, including cybersecurity risks and incidents, and protected systems, so as to ensure the availability, integrity, and reliability thereof;

"(B) communicating or disclosing critical infrastructure information, including cybersecu-

rity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

''(C) voluntarily disseminating critical infrastructure information, including cybersecurity risks and incidents, to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

''(14) INFORMATION SYSTEM.—The term 'information system' has the meaning given the term in section 3502 of title 44, United States Code.

''(15) INTELLIGENCE COMMUNITY.—The term 'intelligence community' has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

''(16) MONITOR.—The term 'monitor' means to acquire, identify, or scan, or to possess, information that is stored on, processed by, or transiting an information system.

"(17) NATIONAL CYBERSECURITY ASSET RESPONSE ACTIVITIES.—The term 'national cybersecurity asset response activities' means—

"(A) furnishing cybersecurity technical assistance to entities affected by cybersecurity risks to protect assets, mitigate vulnerabilities, and reduce impacts of cyber incidents;

"(B) identifying other entities that may be at risk of an incident and assessing risk to the same or similar vulnerabilities;

"(C) assessing potential cybersecurity risks to a sector or region, including potential cascading effects, and developing courses of action to mitigate such risks;

"(D) facilitating information sharing and operational coordination with threat response; and

"(E) providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery from cybersecurity risks.

"(18) NATIONAL SECURITY SYSTEM.—The term 'national security system' has the meaning given the term in section 11103 of title 40, United States Code.

''(19) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' means a Federal department or agency, designated by law or Presidential directive, with responsibility for providing institutional knowledge and specialized expertise of a sector, as well as leading, facilitating, or supporting programs and associated activities of its designated critical infrastructure sector in the all hazards environment in coordination with the Department.

''(20) SECURITY VULNERABILITY.—The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.

''(21) SHARING.—The term 'sharing' (including all conjugations thereof) means providing, receiving, and disseminating (including all conjugations of each such terms).''.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—The Homeland Security Act of 2002 (6 U.S.C. 101 et seq.) is amended—

(1) by amending section 2201 to read as follows:

"SEC. 2201. DEFINITION.

"In this subtitle, the term 'Cybersecurity Advisory Committee' means the advisory committee established under section 2219(a).";

(2) in section 2202—

(A) in subsection (a)(1), by striking "(in this subtitle referred to as the Agency)";

(B) in subsection (f)—

(i) in paragraph (1), by inserting "Executive" before "Assistant Director"; and

(ii) in paragraph (2), by inserting "Executive" before "Assistant Director";

(3) in section 2203(a)(2), by striking "as the 'Assistant Director'" and inserting "as the 'Executive Assistant Director'";

(4) in section 2204(a)(2), by striking "as the 'Assistant Director'" and inserting "as the 'Executive Assistant Director'";

(5) in section 2209—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through subsection (o) as subsections (a) through (n), respectively;

(C) in subsection (c)(1)(A)(iii), as so redesignated, by striking ", as that term is de-

fined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))'';

(D) in subsection (d), as so redesignated, in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)'';

(E) in subsection (j), as so redesignated, by striking ''subsection (c)(8)'' and inserting ''subsection (b)(8)''; and

(F) in subsection (n), as so redesignated—

(i) in paragraph (2)(A), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)''; and

(ii) in paragraph (3)(B)(i), by striking ''subsection (c)(12)'' and inserting ''subsection (b)(12)'';

(6) in section 2210—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (d) as subsections (a) through (c), respectively;

(C) in subsection (b), as so redesignated—

(i) by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Informa-

tion Sharing and Analysis Organizations''; and

(ii) by striking ''(as defined in section 2209)''; and

(D) in subsection (c), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (b)'';

(7) in section 2211, by striking subsection (h);

(8) in section 2212, by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations'';

(9) in section 2213—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (f) as subsections (a) through (e); respectively;

(C) in subsection (b), as so redesignated, by striking ''subsection (b)'' each place it appears and inserting ''subsection (a)'';

(D) in subsection (c), as so redesignated, in the matter preceding paragraph (1), by striking ''subsection (b)'' and inserting ''subsection (a)''; and

(E) in subsection (d), as so redesignated—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(II) in subparagraph (A), by striking ''subsection (c)(1)'' and inserting ''subsection (b)(1)''; and

(III) in subparagraph (B), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)''; and

(ii) in paragraph (2), by striking ''subsection (c)(2)'' and inserting ''subsection (b)(2)'';

(10) in section 2216, as so redesignated—

(A) by striking subsection (a);

(B) by redesignating subsections (b) through (h) as subsections (a) through (g), respectively;

(C) in subsection (a), as so redesignated—

(i) in the matter preceding paragraph (1), by striking ''subsection (e)'' and inserting ''subsection (d)'';

(ii) in paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(iii) in paragraph (2), by striking ''subsection (c)'' and inserting ''subsection (b)'';

(D) in subsection (b)(4), as so redesignated—

(i) by striking ''subsection (e)'' and inserting ''subsection (d)''; and

(ii) by striking ''subsection (h)'' and inserting ''subsection (g)'';

(E) in subsection (d), as so redesignated, by striking ''subsection (b)(1)'' each place it appears and inserting ''subsection (a)(1)'';

(F) in subsection (e), as so redesignated—

(i) by striking ''subsection (b)'' and inserting ''subsection (a)'';

(ii) by striking ''subsection (e)'' and inserting ''subsection (d)''; and

(iii) by striking ''subsection (b)(1)'' and inserting ''subsection (a)(1)''; and

(G) in subsection (f), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (b)'';

(11) in section 2217, as so redesignated, by striking subsection (f) and inserting the following:

''(f) CYBER DEFENSE OPERATION DEFINED.—In this section, the term 'cyber defense operation' means the use of a defensive measure.''; and

(12) in section 2222—

(A) by striking paragraphs (3), (5), and (8);

(B) by redesignating paragraph (4) as paragraph (3); and

(C) by redesignating paragraphs (6) and (7) as paragraphs (4) and (5), respectively.

(c) TABLE OF CONTENTS AMENDMENTS.—The table of contents in section 1(b) of the Homeland Security Act of 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

(1) by inserting before the item relating to subtitle A of title XXII the following:

''Sec. 2200. Definitions.'';

(2) by striking the item relating to section 2201 and insert the following:

''Sec. 2201. Definition.''; and

(3) by striking the second item relating to section 2215 and all that follows through the item relating to section 2217 and inserting the following:

''Sec. 2216. Cybersecurity State Coordinator.

(d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—Section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501) is amended—

(1) by striking paragraphs (4) through (7) and inserting the following:

''(4) CYBERSECURITY PURPOSE.—The term 'cybersecurity purpose' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(5) CYBERSECURITY THREAT.—The term 'cybersecurity threat' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(6) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

''(7) DEFENSIVE MEASURE.—The term 'defensive measure' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) by striking paragraph (13) and inserting the following:

''(13) MONITOR.— The term 'monitor' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''; and

(3) by striking paragraph (17) and inserting the following:

''(17) SECURITY VULNERABILITY.—The term 'security vulnerability' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.''.

SEC. 4. ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.

(a) FEDERAL CYBERSECURITY ENHANCEMENT ACT OF 2015.—The Federal Cybersecurity Enhancement Act of 2015 (6 U.S.C. 1521 et seq.) is amended—

(1) in section 222 (6 U.S.C. 1521)—

(A) in paragraph (2), by striking ''section 2210'' and inserting ''section 2200''; and

(B) in paragraph (4), by striking ''section 2209'' and inserting ''section 2200'';

(2) in section 223 (6 U.S.C. 151 note) is amended by striking ''section 2213(b)(1)'' each place it appears and inserting ''section 2213(a)(1)'';

(3) in section 226—

(A) in subsection (a)—

(i) in paragraph (1), by striking ''section 2213'' and inserting ''section 2200'';

(ii) in paragraph (4), by striking ''section 2210(b)(1)'' and inserting ''section 2210(a)(1)''; and

(iii) in paragraph (5), by striking ''section 2213(b)'' and inserting ''section 2213(a)''; and

(B) in subsection (c)(1)(A)(vi), by striking ''section 2213(c)(5)'' and inserting ''section 2213(b)(5)''; and

(4) in section 227(b) (6 U.S.C. 1525(b)), by striking ''section 2213(d)(2)'' and inserting ''section 2213(c)(2)''.

(b) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking ''section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))'' and inserting ''section 2210(c) of the Homeland Security Act of 2002''.

(c) WILLIAM M. (MAC) THORNBERRY NATIONAL DEFENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—Section 9002 of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a) is amended—

(1) in subsection (a)—

(A) in paragraph (5), by striking ''section 2222(5) of the Homeland Security Act of 2002 (6 U.S.C. 671(5))'' and inserting ''section 2200 of the Homeland Security Act of 2002''; and

(B) by amending paragraph (7) to read as follows:

''(7) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.'';

(2) in subsection (c)(3)(B), by striking ''section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. 651(5))'' and inserting ''section 2200 of the Homeland Security Act of 2002''; and

(3) in subsection (d)—

(A) by striking ''section 2215'' and inserting ''2218''; and

(B) by striking '', as added by this section''.

(d) NATIONAL SECURITY ACT OF 1947.—Section 113B of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking section ''226 of the Homeland Security Act of 2002 (6 U.S.C. 147)'' and in-

serting ''section 2206 of the Homeland Security Act of 2002''.

(e) IOT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c) is amended by striking ''section 2209(m)'' and inserting ''section 2209(l)''.

(f) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of the Small Business Act (15 U.S.C. 648(a)(8)(B)) is amended by striking ''section 2209(a)'' and inserting ''section 2200''.

(g) TITLE 46.—Section 70101(2) of title 46, United States Code, is amended by striking ''section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148)'' and inserting ''section 2200 of the Homeland Security Act of 2002''.