

Calendar No. **632**117TH CONGRESS
2^D SESSION**S. 2540****[Report No. 117-248]**

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

 IN THE SENATE OF THE UNITED STATES

JULY 29, 2021

Mr. PORTMAN (for himself, Mr. PETERS, and Ms. HASSAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 13, 2022

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

A BILL

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

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “CISA Technical Cor-
5 rections and Improvements Act of 2021”.

1 **SEC. 2. REDESIGNATIONS.**

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

5 (1) by striking section 2201 (6 U.S.C. 651);

6 (2) by redesignating sections 2202 through
7 2214 as sections 2201 through 2213, respectively;

8 (3) by redesignating section 2217 (6 U.S.C.
9 665f) as section 2219;

10 (4) by redesignating section 2216 (6 U.S.C.
11 665e) as section 2218;

12 (5) by redesignating the fourth section 2215
13 (relating to Sector Risk Management Agencies) (6
14 U.S.C. 665d) as section 2217;

15 (6) by redesignating the third section 2215 (re-
16 lating to the Cybersecurity State Coordinator) (6
17 U.S.C. 665e) as section 2216; and

18 (7) by redesignating the first section 2215 (re-
19 lating to Duties and Authorities Relating to .GOV
20 Internet Domain) (6 U.S.C. 665) as section 2214.

21 (b) **TECHNICAL AND CONFORMING AMENDMENTS.**—

22 The Homeland Security Act of 2002 (6 U.S.C. 101 et
23 seq.) is amended—

24 (1) in section 220(d)(3)(C) (6 U.S.C.
25 195f(d)(3)(C)) by striking “section 2201” and in-
26 serting “section 2200”;

1 (2) in section 846(1) (6 U.S.C. 417(1)), by
2 striking “section 2209” and inserting “section
3 2208”;

4 (3) in section 1801(e)(16) (6 U.S.C.
5 571(e)(16)) by striking “section 2202(e)(7)” and in-
6 serting “section 2201(e)(7)”;

7 (4) in section 2001(4)(A)(iii)(H) (6 U.S.C.
8 601(4)(A)(iii)(H)), by striking “section 2214(a)(2)”
9 and inserting “section 2213(a)(2)”;

10 (5) in section 2008(a)(3) (6 U.S.C. 609(a)(3)),
11 by striking “section 2214(a)(2)” and inserting “sec-
12 tion 2213(a)(2);”

13 (6) in section 2201, as so redesignated—

14 (A) in subsection (e)—

15 (i) in the first paragraph (12), by
16 striking “section 2215” and inserting “sec-
17 tion 2216”;

18 (ii) by redesignating the second and
19 third paragraphs (12) as paragraphs (13)
20 and (14), respectively; and

21 (iii) in paragraph (13), as so redesi-
22 gnated, by striking “section 2215” and in-
23 serting “section 2214”; and

1 (B) in subsection (c)(2), by striking “sec-
2 tions 2203(b) and 2204(b)” and inserting “sec-
3 tions 2202(b) and 2203(b)”;

4 (7) in section 2202(b)(3), as so redesignated,
5 by striking “section 2202(e)(7)” and inserting “sec-
6 tion 2201(e)(7)”;

7 (8) in section 2203(b)(3), as so redesignated,
8 by striking “section 2202(e)(7)” and inserting “sec-
9 tion 2201(e)(7)”;

10 (9) in section 2204, as so redesignated, in the
11 matter preceding paragraph (1), by striking “section
12 2202” and inserting “section 2201”;

13 (10) in section 2210(b)(2)(A), as so redesi-
14 gnated, by striking “section 2209” and inserting
15 “section 2208”; and

16 (11) in section 2217(e)(4)(A), by striking “sec-
17 tion 2209” and inserting “section 2208”.

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

21 (1) by striking inserting before the item relat-
22 ing to subtitle A of title XXII the following:

“Sec. 2200. Definitions.”;

23 and

24 (2) by striking the items relating to sections
25 2201 through 2217 and inserting the following:

“Sec. 2201. Cybersecurity and Infrastructure Security Agency.
 “Sec. 2202. Cybersecurity Division.
 “Sec. 2203. Infrastructure Security Division.
 “Sec. 2204. Enhancement of Federal and non-Federal cybersecurity.
 “Sec. 2205. Net guard.
 “Sec. 2206. Cyber Security Enhancement Act of 2002.
 “Sec. 2207. Cybersecurity recruitment and retention.
 “Sec. 2208. National cybersecurity and communications integration center.
 “Sec. 2209. Cybersecurity plans.
 “Sec. 2210. Cybersecurity strategy.
 “Sec. 2211. Clearances.
 “Sec. 2212. Federal intrusion detection and prevention system.
 “Sec. 2213. National Asset Database.
 “Sec. 2214. Duties and authorities relating to .gov internet domain.
 “Sec. 2215. Joint Cyber Planning Office.
 “Sec. 2216. Cybersecurity State Coordinator.
 “Sec. 2217. Sector Risk Management Agencies.
 “Sec. 2218. Cybersecurity Advisory Committee.
 “Sec. 2219. Cybersecurity education and training programs.”.

1 (d) **ADDITIONAL TECHNICAL AMENDMENT.**—

2 (1) **AMENDMENT.**—Section 904(b)(1) of the
 3 DOTGOV Act of 2020 (title IX of division U of
 4 Public Law 116–260) is amended, in the matter pre-
 5 ceding subparagraph (A), by striking “Homeland
 6 Security Act” and inserting “Homeland Security Act
 7 of 2002”.

8 (2) **EFFECTIVE DATE.**—The amendment made
 9 by paragraph (1) shall take effect as if enacted as
 10 part of the DOTGOV Act of 2020 (title IX of divi-
 11 sion U of Public Law 116–260).

12 **SEC. 3. CONSOLIDATION OF DEFINITIONS.**

13 (a) **IN GENERAL.**—Title XXII of the Homeland Se-
 14 curity Act of 2002 (6 U.S.C. 651) is amended—

15 (1) by striking section 2201; and

1 (2) by inserting before the subtitle A heading
2 the following:

3 **“SEC. 2200. DEFINITIONS.**

4 “Except as otherwise specifically provided, in this
5 title:

6 “(1) AGENCY.—The term ‘Agency’ means the
7 Cybersecurity and Infrastructure Security Agency.

8 “(2) AGENCY INFORMATION.—The term ‘agen-
9 cy information’ means information collected or main-
10 tained by or on behalf of an agency.

11 “(3) AGENCY INFORMATION SYSTEM.—The
12 term ‘agency information system’ means an informa-
13 tion system used or operated by an agency or by an-
14 other entity on behalf of an agency.

15 “(4) APPROPRIATE CONGRESSIONAL COMMIT-
16 TEES.—The term ‘appropriate congressional com-
17 mittees’ means—

18 “(A) the Committee on Homeland Security
19 and Governmental Affairs of the Senate; and

20 “(B) the Committee on Homeland Security
21 of the House of Representatives.

22 “(5) CRITICAL INFRASTRUCTURE INFORMA-
23 TION.—The term ‘critical infrastructure information’
24 means information not customarily in the public do-

1 main and related to the security of critical infra-
2 structure or protected systems—

3 “(A) actual, potential, or threatened inter-
4 ference with, attack on, compromise of, or inca-
5 pacitation of critical infrastructure or protected
6 systems by either physical or computer-based
7 attack or other similar conduct (including the
8 misuse of or unauthorized access to all types of
9 communications and data transmission systems)
10 that violates Federal, State, or local law, harms
11 interstate commerce of the United States, or
12 threatens public health or safety;

13 “(B) the ability of any critical infrastruc-
14 ture or protected system to resist such inter-
15 ference, compromise, or incapacitation, includ-
16 ing any planned or past assessment, projection,
17 or estimate of the vulnerability of critical infra-
18 structure or a protected system, including secu-
19 rity testing, risk evaluation thereto, risk man-
20 agement planning, or risk audit; or

21 “(C) any planned or past operational prob-
22 lem or solution regarding critical infrastructure
23 or protected systems, including repair, recovery,
24 reconstruction, insurance, or continuity; to the

1 extent it is related to such interference, com-
2 promise, or incapacitation.

3 ~~“(6) CYBER THREAT INDICATOR.—~~The term
4 ‘cyber threat indicator’ means information that is
5 necessary to describe or identify—

6 ~~“(A) malicious reconnaissance, including~~
7 ~~anomalous patterns of communications that ap-~~
8 ~~pear to be transmitted for the purpose of gath-~~
9 ~~ering technical information related to a cyberse-~~
10 ~~curity threat or security vulnerability;~~

11 ~~“(B) a method of defeating a security con-~~
12 ~~trol or exploitation of a security vulnerability;~~

13 ~~“(C) a security vulnerability, including~~
14 ~~anomalous activity that appears to indicate the~~
15 ~~existence of a security vulnerability;~~

16 ~~“(D) a method of causing a user with le-~~
17 ~~gitimate access to an information system or in-~~
18 ~~formation that is stored on, processed by, or~~
19 ~~transiting an information system to unwittingly~~
20 ~~enable the defeat of a security control or exploi-~~
21 ~~tation of a security vulnerability;~~

22 ~~“(E) malicious cyber command and con-~~
23 ~~trol;~~

24 ~~“(F) the actual or potential harm caused~~
25 ~~by an incident, including a description of the in-~~

1 formation exfiltrated as a result of a particular
2 cybersecurity threat;

3 “(G) any other attribute of a cybersecurity
4 threat, if disclosure of such attribute is not oth-
5 erwise prohibited by law; or

6 “(H) any combination thereof.

7 “(7) CYBERSECURITY PURPOSE.—The term ‘cy-
8 bersecurity purpose’ means the purpose of protecting
9 an information system or information that is stored
10 on, processed by, or transiting an information sys-
11 tem from a cybersecurity threat or security vulner-
12 ability.

13 “(8) CYBERSECURITY RISK.—The term ‘cyber-
14 security risk’—

15 “(A) means threats to and vulnerabilities
16 of information or information systems and any
17 related consequences caused by or resulting
18 from unauthorized access, use, disclosure, deg-
19 radation, disruption, modification, or destruc-
20 tion of such information or information sys-
21 tems, including such related consequences
22 caused by an act of terrorism; and

23 “(B) does not include any action that sole-
24 ly involves a violation of a consumer term of
25 service or a consumer licensing agreement.

1 “(9) CYBERSECURITY THREAT.—

2 “(A) IN GENERAL.—Except as provided in
3 subparagraph (B), the term ‘cybersecurity
4 threat’ means an action, not protected by the
5 First Amendment to the Constitution of the
6 United States, on or through an information
7 system that may result in an unauthorized ef-
8 fort to adversely impact the security, avail-
9 ability, confidentiality, or integrity of an infor-
10 mation system or information that is stored on,
11 processed by, or transiting an information sys-
12 tem.

13 “(B) EXCLUSION.—The term ‘cybersecu-
14 rity threat’ does not include any action that
15 solely involves a violation of a consumer term of
16 service or a consumer licensing agreement.

17 “(10) DEFENSIVE MEASURE.—

18 “(A) IN GENERAL.—Except as provided in
19 subparagraph (B), the term ‘defensive measure’
20 means an action, device, procedure, signature,
21 technique, or other measure applied to an infor-
22 mation system or information that is stored on,
23 processed by, or transiting an information sys-
24 tem that detects, prevents, or mitigates a

1 known or suspected cybersecurity threat or se-
2 curity vulnerability.

3 “(B) EXCLUSION.—The term ‘defensive
4 measure’ does not include a measure that de-
5 stroys, renders unusable, provides unauthorized
6 access to, or substantially harms an information
7 system or information stored on, processed by,
8 or transiting such information system not
9 owned by—

10 “(i) the entity operating the measure;

11 or

12 “(ii) another entity or Federal entity
13 that is authorized to provide consent and
14 has provided consent to that private entity
15 for operation of such measure.

16 “(11) HOMELAND SECURITY ENTERPRISE.—

17 The term ‘Homeland Security Enterprise’ means rel-
18 evant governmental and nongovernmental entities in-
19 volved in homeland security, including Federal,
20 State, local, and tribal government officials, private
21 sector representatives, academics, and other policy
22 experts.

23 “(12) INCIDENT.—The term ‘incident’ means
24 an occurrence that actually or imminently jeopard-
25 izes, without lawful authority, the integrity, con-

1 confidentiality, or availability of information on an in-
2 formation system; or actually or imminently jeopard-
3 izes, without lawful authority, an information sys-
4 tem.

5 “(13) INFORMATION SHARING AND ANALYSIS
6 ORGANIZATION.—The term ‘Information Sharing
7 and Analysis Organization’ means any formal or in-
8 formal entity or collaboration created or employed by
9 public or private sector organizations, for purposes
10 of—

11 “(A) gathering and analyzing critical infra-
12 structure information, including information re-
13 lated to cybersecurity risks and incidents, in
14 order to better understand security problems
15 and interdependencies related to critical infra-
16 structure, including cybersecurity risks and in-
17 cidents, and protected systems, so as to ensure
18 the availability, integrity, and reliability thereof;

19 “(B) communicating or disclosing critical
20 infrastructure information, including cybersecu-
21 rity risks and incidents, to help prevent, detect,
22 mitigate, or recover from the effects of a inter-
23 ference, compromise, or a incapacitation prob-
24 lem related to critical infrastructure, including

1 cybersecurity risks and incidents, or protected
2 systems; and

3 “(C) voluntarily disseminating critical in-
4 frastructure information, including cybersecu-
5 rity risks and incidents, to its members, State,
6 local, and Federal Governments, or any other
7 entities that may be of assistance in carrying
8 out the purposes specified in subparagraphs (A)
9 and (B).

10 “(14) INFORMATION SYSTEM.—The term ‘infor-
11 mation system’ has the meaning given the term in
12 section 3502 of title 44, United States Code.

13 “(15) INTELLIGENCE COMMUNITY.—The term
14 ‘intelligence community’ has the meaning given the
15 term in section 3(4) of the National Security Act of
16 1947 (50 U.S.C. 3003(4)).

17 “(16) MONITOR.—The term ‘monitor’ means to
18 acquire, identify, or scan, or to possess, information
19 that is stored on, processed by, or transiting an in-
20 formation system.

21 “(17) NATIONAL CYBERSECURITY ASSET RE-
22 SPONSE ACTIVITIES.—The term ‘national cybersecu-
23 rity asset response activities’ means—

24 “(A) furnishing cybersecurity technical as-
25 sistance to entities affected by cybersecurity

1 risks to protect assets, mitigate vulnerabilities,
2 and reduce impacts of cyber incidents;

3 ~~“(B) identifying other entities that may be~~
4 ~~at risk of an incident and assessing risk to the~~
5 ~~same or similar vulnerabilities;~~

6 ~~“(C) assessing potential cybersecurity risks~~
7 ~~to a sector or region, including potential cas-~~
8 ~~cading effects, and developing courses of action~~
9 ~~to mitigate such risks;~~

10 ~~“(D) facilitating information sharing and~~
11 ~~operational coordination with threat response;~~
12 ~~and~~

13 ~~“(E) providing guidance on how best to~~
14 ~~utilize Federal resources and capabilities in a~~
15 ~~timely, effective manner to speed recovery from~~
16 ~~cybersecurity risks.~~

17 ~~“(18) NATIONAL SECURITY SYSTEM.—The term~~
18 ~~‘national security system’ has the meaning given the~~
19 ~~term in section 11103 of title 40, United States~~
20 ~~Code.~~

21 ~~“(19) SECTOR RISK MANAGEMENT AGENCY.—~~
22 ~~The term ‘Sector Risk Management Agency’ means~~
23 ~~a Federal department or agency, designated by law~~
24 ~~or Presidential directive, with responsibility for pro-~~
25 ~~viding institutional knowledge and specialized exper-~~

1 tise of a sector, as well as leading, facilitating, or
 2 supporting programs and associated activities of its
 3 designated critical infrastructure sector in the all
 4 hazards environment in coordination with the De-
 5 partment.

6 “(20) SECURITY VULNERABILITY.—The term
 7 ‘security vulnerability’ means any attribute of hard-
 8 ware, software, process, or procedure that could en-
 9 able or facilitate the defeat of a security control.

10 “(21) SHARING.—The term ‘sharing’ (including
 11 all conjugations thereof) means providing, receiving,
 12 and disseminating (including all conjugations of each
 13 such terms).”.

14 (b) TECHNICAL AND CONFORMING AMENDMENTS.—

15 The Homeland Security Act of 2002 (6 U.S.C. 101 et
 16 seq.) is amended—

17 (1) in section 2201, as so redesignated—

18 (A) in subsection (a)(1), by striking “(in
 19 this subtitle referred to as the Agency)”;

20 (B) in subsection (f)—

21 (i) in paragraph (1), by inserting
 22 “Executive” before “Assistant Director”;
 23 and

24 (ii) in paragraph (2), by inserting
 25 “Executive” before “Assistant Director”;

1 (2) in section 2202(a)(2), as so redesignated,
2 by striking “as the ‘Assistant Director’” and insert-
3 ing “as the ‘Executive Assistant Director’”;

4 (3) in section 2203(a)(2), as so redesignated,
5 by striking “as the ‘Assistant Director’” and insert-
6 ing “as the ‘Executive Assistant Director’”;

7 (4) in section 2208, as so redesignated—

8 (A) by striking subsection (a);

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

12 (C) in subsection (c)(1)(A)(iii), as so re-
13 designated, by striking “, as that term is de-
14 fined under section 3(4) of the National Secu-
15 rity Act of 1947 (50 U.S.C. 3003(4))”;

16 (D) in subsection (d), as so redesignated,
17 in the matter preceding paragraph (1), by strik-
18 ing “subsection (c)” and inserting “subsection
19 (b)”;

20 (E) in subsection (j), as so redesignated,
21 by striking “subsection (c)(8)” and inserting
22 “subsection (b)(8)”; and

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

1 (i) in paragraph (2)(A), by striking
2 “subsection (e)(12)” and inserting “sub-
3 section (b)(12)”; and

4 (ii) in paragraph (3)(B)(i), by striking
5 “subsection (e)(12)” and inserting “sub-
6 section (b)(12)”;

7 (5) in section 2209, as so redesignated—

8 (A) by striking subsection (a);

9 (B) by redesignating subsections (b)
10 through (d) as subsections (a) through (c), re-
11 spectively;

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

13 (i) by striking “information sharing
14 and analysis organizations (as defined in
15 section 2222(5))” and inserting “Informa-
16 tion Sharing and Analysis Organizations”;
17 and

18 (ii) by striking “(as defined in section
19 2209)”; and

20 (D) in subsection (c), as so redesignated,
21 by striking “subsection (c)” and inserting “sub-
22 section (b)”;

23 (6) in section 2210, as so redesignated, by
24 striking subsection (h);

1 (7) in section 2211, as so redesignated, by
2 striking “information sharing and analysis organiza-
3 tions (as defined in section 2222(5))” and inserting
4 “Information Sharing and Analysis Organizations”;

5 (8) in section 2212, as so redesignated—

6 (A) by striking subsection (a);

7 (B) by redesignating subsections (b)
8 through (f) as subsections (a) through (e); re-
9 spectively;

10 (C) in subsection (b), as so redesignated,
11 by striking “subsection (b)” each place it ap-
12 pears and inserting “subsection (a)”;

13 (D) in subsection (c), as so redesignated,
14 in the matter preceding paragraph (1), by strik-
15 ing “subsection (b)” and inserting “subsection
16 (a)”;

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

18 (i) in paragraph (1)—

19 (I) in the matter preceding sub-
20 paragraph (A), by striking “sub-
21 section (c)(2)” and inserting “sub-
22 section (b)(2)”;

23 (II) in subparagraph (A), by
24 striking “subsection (c)(1)” and in-
25 serting “subsection (b)(1)”;

1 (III) in subparagraph (B), by
2 striking “subsection (e)(2)” and in-
3 serting “subsection (b)(2)”; and

4 (ii) in paragraph (2), by striking
5 “subsection (e)(2)” and inserting “sub-
6 section (b)(2)”;

7 (9) in section 2215 (6 U.S.C. 665b)—

8 (A) by striking subsection (a);

9 (B) by redesignating subsections (b)
10 through (h) as subsections (a) through (g), re-
11 spectively;

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

13 (i) in the matter preceding paragraph
14 (1), by striking “subsection (e)” and in-
15 serting “subsection (d)”;

16 (ii) in paragraph (1), by striking
17 “subsection (e)” and inserting “subsection
18 (b)”; and

19 (iii) in paragraph (2), by striking
20 “subsection (e)” and inserting “subsection
21 (b)”;

22 (D) in subsection (b)(4), as so redesi-
23 gnated—

24 (i) by striking “subsection (e)” and
25 inserting “subsection (d)”; and

1 (ii) by striking “subsection (h)” and
2 inserting “subsection (g)”;
3 (F) in subsection (d), as so redesignated,
4 by striking “subsection (b)(1)” each place it ap-
5 pears and inserting “subsection (a)(1)”;
6 (F) in subsection (e), as so redesignated—
7 (i) by striking “subsection (b)” and
8 inserting “subsection (a)”;
9 (ii) by striking “subsection (e)” and
10 inserting “subsection (d)”; and
11 (iii) by striking “subsection (b)(1)”
12 and inserting “subsection (a)(1)”; and
13 (G) in subsection (f), as so redesignated,
14 by striking “subsection (e)” and inserting “sub-
15 section (b)”;
16 (10) in section 2216, as so redesignated, by
17 striking subsection (f) and inserting the following:
18 “(f) CYBER DEFENSE OPERATION DEFINED.—In
19 this section, the term ‘cyber defense operation’ means the
20 use of a defensive measure.”; and
21 (11) in section 2222—
22 (A) by striking paragraphs (3), (5), and
23 (8);
24 (B) by redesignating paragraph (4) as
25 paragraph (3); and

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

3 (e) ~~CYBERSECURITY ACT OF 2015 DEFINITIONS.~~—

4 Section 102 of the ~~Cybersecurity Act of 2015~~ (6 U.S.C.
5 1501) is amended—

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

8 “(4) ~~CYBERSECURITY PURPOSE.~~—The term ‘cy-
9 bersecurity purpose’ has the meaning given the term
10 in section 2200 of the Homeland Security Act of
11 2002.

12 “(5) ~~CYBERSECURITY THREAT.~~—The term ‘cy-
13 bersecurity threat’ has the meaning given the term
14 in section 2200 of the Homeland Security Act of
15 2002.

16 “(6) ~~CYBER THREAT INDICATOR.~~—The term
17 ‘cyber threat indicator’ has the meaning given the
18 term in section 2200 of the Homeland Security Act
19 of 2002.

20 “(7) ~~DEFENSIVE MEASURE.~~—The term ‘defen-
21 sive measure’ has the meaning given the term in sec-
22 tion 2200 of the Homeland Security Act of 2002.”;

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

1 “(13) MONITOR.— The term ‘monitor’ has the
2 meaning given the term in section 2200 of the
3 Homeland Security Act of 2002.”; and

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

6 “(17) SECURITY VULNERABILITY.—The term
7 ‘security vulnerability’ has the meaning given the
8 term in section 2200 of the Homeland Security Act
9 of 2002.”.

10 **SEC. 4. ADDITIONAL TECHNICAL AND CONFORMING**
11 **AMENDMENTS.**

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

15 (1) in section 222 (6 U.S.C. 1521)—

16 (A) in paragraph (2), by striking “section
17 2210” and inserting “section 2200”; and

18 (B) in paragraph (4), by striking “section
19 2209” and inserting “section 2200”;

20 (2) in section 223 (6 U.S.C. 151 note) is
21 amended by striking “section 2213(b)(1)” each place
22 it appears and inserting “section 2212(a)(1)”; and

23 (3) in section 226—

24 (A) in subsection (a)—

1 (i) in paragraph (1), by striking “sec-
2 tion 2213” and inserting “section 2200”;

3 (ii) in paragraph (4), by striking “sec-
4 tion 2210(b)(1)” and inserting “section
5 2209(a)(1)”; and

6 (iii) in paragraph (5), by striking
7 “section 2213(b)” and inserting “section
8 2212(a)”; and

9 (B) in subsection (e)(1)(A)(vi), by striking
10 “section 2213(e)(5)” and inserting “section
11 2212(b)(5)”; and

12 (4) in section 227 (6 U.S.C. 1525)—

13 (A) in subsection (a), by striking “section
14 2213” and inserting “section 2212”; and

15 (B) in subsection (b), by striking “section
16 2213(d)(2)” and inserting “section
17 2212(e)(2)”.

18 (b) PUBLIC HEALTH SERVICE ACT.—Section
19 2811(b)(4)(D) of the Public Health Service Act (42
20 U.S.C. 300hh–10(b)(4)(D)) is amended by striking “sec-
21 tion 228(e) of the Homeland Security Act of 2002 (6
22 U.S.C. 149(e))” and inserting “section 2209(e) of the
23 Homeland Security Act of 2002”.

24 (c) WILLIAM M. (MAC) THORNBERRY NATIONAL DE-
25 FENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—

1 Section 9002 of the William M. (Mac) Thornberry Na-
2 tional Defense Authorization Act for Fiscal Year 2021 (6
3 U.S.C. 652a) is amended—

4 (1) in subsection (a)—

5 (A) in paragraph (5), by striking “section
6 2222(5) of the Homeland Security Act of 2002
7 (6 U.S.C. 671(5))” and inserting “section 2200
8 of the Homeland Security Act of 2002”; and

9 (B) in paragraph (7), by striking “given
10 the term” and all that follows and inserting
11 “given the term in section 2200 of the Home-
12 land Security Act of 2002”;

13 (2) in subsection (b)(1)(A), by striking “section
14 2202(e)(4) of the Homeland Security Act (6 U.S.C.
15 652(e)(4))” and inserting “section 2201(e)(4)”;

16 (3) in subsection (c)(3)(B), by striking “section
17 2201(5) of the Homeland Security Act of 2002 (6
18 U.S.C. 651(5))” and inserting “section 2200 of the
19 Homeland Security Act of 2002”; and

20 (4) in subsection (d)—

21 (A) by striking “section 2215” and insert-
22 ing “2217”; and

23 (B) by striking “, as added by this sec-
24 tion”.

1 (d) NATIONAL SECURITY ACT OF 1947.—Section
2 113B of the National Security Act of 1947 (50 U.S.C.
3 3049a(b)(4)) is amended by striking section “226 of the
4 Homeland Security Act of 2002 (6 U.S.C. 147)” and in-
5 serting “section 2207 of the Homeland Security Act of
6 2002”.

7 (e) CYBERSECURITY ACT OF 2015.—Section 404(a)
8 of the Cybersecurity Act of 2015 (6 U.S.C. 1532(a)) is
9 amended by striking “section 2209” and inserting “sec-
10 tion 2208”.

11 (f) IOT CYBERSECURITY IMPROVEMENT ACT OF
12 2020.—Section 5(b)(3) of the IoT Cybersecurity Improve-
13 ment Act of 2020 (15 U.S.C. 278g–3e) is amended by
14 striking “section 2209(m)” and inserting “section
15 2208(l)”.

16 (g) SMALL BUSINESS ACT.—Section 21(a)(8)(B) of
17 the Small Business Act (15 U.S.C. 648(a)(8)(B)) is
18 amended by striking “section 2209(a)” and inserting “sec-
19 tion 2200”.

20 (h) TITLE 46.—Section 70101(2) of title 46, United
21 States Code, is amended by striking “section 227 of the
22 Homeland Security Act of 2002 (6 U.S.C. 148)” and in-
23 serting “section 2200 of the Homeland Security Act of
24 2002”.

1 **SECTION 1. SHORT TITLE.**

2 *This Act may be cited as the “CISA Technical Correc-*
3 *tions and Improvements Act of 2021”.*

4 **SEC. 2. REDESIGNATIONS.**

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

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

10 (2) *by redesignating section 2216 (6 U.S.C.*
11 *665e) as section 2219;*

12 (3) *by redesignating the fourth section 2215 (re-*
13 *lating to Sector Risk Management Agencies) (6*
14 *U.S.C. 665d) as section 2218;*

15 (4) *by redesignating the third section 2215 (re-*
16 *lating to the Cybersecurity State Coordinator) (6*
17 *U.S.C. 665c) as section 2217; and*

18 (5) *by redesignating the second section 2215 (re-*
19 *lating to the Joint Cyber Planning Office) (6 U.S.C.*
20 *665b) as section 2216.*

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

24 (1) *in paragraph (11), by striking “and” at the*
25 *end;*

26 (2) *in the first paragraph (12)—*

1 (A) by striking “section 2215” and insert-
2 ing “section 2217”; and

3 (B) by striking “and” at the end; and

4 (3) by redesignating the second and third para-
5 graphs (12) as paragraphs (13) and (14), respec-
6 tively.

7 (c) *ADDITIONAL TECHNICAL AMENDMENT.*—

8 (1) *AMENDMENT.*—Section 904(b)(1) of the
9 *DOTGOV Act of 2020 (title IX of division U of Pub-*
10 *lic Law 116–260)* is amended, in the matter pre-
11 ceding subparagraph (A), by striking “Homeland Se-
12 curity Act” and inserting “Homeland Security Act of
13 2002”.

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

18 **SEC. 3. CONSOLIDATION OF DEFINITIONS.**

19 (a) *IN GENERAL.*—Title XXII of the *Homeland Secu-*
20 *urity Act of 2002 (6 U.S.C. 651)* is amended by inserting
21 before the subtitle A heading the following:

22 **“SEC. 2200. DEFINITIONS.**

23 “Except as otherwise specifically provided, in this
24 title:

1 “(1) *AGENCY*.—The term ‘Agency’ means the Cy-
2 bersecurity and Infrastructure Security Agency.

3 “(2) *AGENCY INFORMATION*.—The term ‘agency
4 information’ means information collected or main-
5 tained by or on behalf of an agency.

6 “(3) *AGENCY INFORMATION SYSTEM*.—The term
7 ‘agency information system’ means an information
8 system used or operated by an agency or by another
9 entity on behalf of an agency.

10 “(4) *APPROPRIATE CONGRESSIONAL COMMIT-*
11 *TEES*.—The term ‘appropriate congressional commit-
12 tees’ means—

13 “(A) the Committee on Homeland Security
14 and Governmental Affairs of the Senate; and

15 “(B) the Committee on Homeland Security
16 of the House of Representatives.

17 “(5) *CRITICAL INFRASTRUCTURE INFORMA-*
18 *TION*.—The term ‘critical infrastructure information’
19 means information not customarily in the public do-
20 main and related to the security of critical infrastruc-
21 ture or protected systems—

22 “(A) actual, potential, or threatened inter-
23 ference with, attack on, compromise of, or inca-
24 pacitation of critical infrastructure or protected
25 systems by either physical or computer-based at-

1 *tack or other similar conduct (including the mis-*
2 *use of or unauthorized access to all types of com-*
3 *munications and data transmission systems)*
4 *that violates Federal, State, or local law, harms*
5 *interstate commerce of the United States, or*
6 *threatens public health or safety;*

7 *“(B) the ability of any critical infrastruc-*
8 *ture or protected system to resist such inter-*
9 *ference, compromise, or incapacitation, includ-*
10 *ing any planned or past assessment, projection,*
11 *or estimate of the vulnerability of critical infra-*
12 *structure or a protected system, including secu-*
13 *rity testing, risk evaluation thereto, risk manage-*
14 *ment planning, or risk audit; or*

15 *“(C) any planned or past operational prob-*
16 *lem or solution regarding critical infrastructure*
17 *or protected systems, including repair, recovery,*
18 *reconstruction, insurance, or continuity, to the*
19 *extent it is related to such interference, com-*
20 *promise, or incapacitation.*

21 *“(6) CYBER THREAT INDICATOR.—The term*
22 *‘cyber threat indicator’ means information that is*
23 *necessary to describe or identify—*

24 *“(A) malicious reconnaissance, including*
25 *anomalous patterns of communications that ap-*

1 *pear to be transmitted for the purpose of gath-*
2 *ering technical information related to a cyberse-*
3 *curity threat or security vulnerability;*

4 *“(B) a method of defeating a security con-*
5 *trol or exploitation of a security vulnerability;*

6 *“(C) a security vulnerability, including*
7 *anomalous activity that appears to indicate the*
8 *existence of a security vulnerability;*

9 *“(D) a method of causing a user with legiti-*
10 *mate access to an information system or infor-*
11 *mation that is stored on, processed by, or*
12 *transiting an information system to unwittingly*
13 *enable the defeat of a security control or exploi-*
14 *tation of a security vulnerability;*

15 *“(E) malicious cyber command and control;*

16 *“(F) the actual or potential harm caused by*
17 *an incident, including a description of the infor-*
18 *mation exfiltrated as a result of a particular cy-*
19 *bersecurity threat;*

20 *“(G) any other attribute of a cybersecurity*
21 *threat, if disclosure of such attribute is not other-*
22 *wise prohibited by law; or*

23 *“(H) any combination thereof.*

24 *“(7) CYBERSECURITY PURPOSE.—The term ‘cy-*
25 *bersecurity purpose’ means the purpose of protecting*

1 *an information system or information that is stored*
2 *on, processed by, or transiting an information system*
3 *from a cybersecurity threat or security vulnerability.*

4 “(8) *CYBERSECURITY RISK.*—*The term ‘cyberse-*
5 *curity risk’—*

6 “(A) *means threats to and vulnerabilities of*
7 *information or information systems and any re-*
8 *lated consequences caused by or resulting from*
9 *unauthorized access, use, disclosure, degradation,*
10 *disruption, modification, or destruction of such*
11 *information or information systems, including*
12 *such related consequences caused by an act of*
13 *terrorism; and*

14 “(B) *does not include any action that solely*
15 *involves a violation of a consumer term of service*
16 *or a consumer licensing agreement.*

17 “(9) *CYBERSECURITY THREAT.*—

18 “(A) *IN GENERAL.*—*Except as provided in*
19 *subparagraph (B), the term ‘cybersecurity threat’*
20 *means an action, not protected by the First*
21 *Amendment to the Constitution of the United*
22 *States, on or through an information system that*
23 *may result in an unauthorized effort to adversely*
24 *impact the security, availability, confidentiality,*
25 *or integrity of an information system or infor-*

1 *mation that is stored on, processed by, or*
2 *transiting an information system.*

3 “(B) *EXCLUSION.*—*The term ‘cybersecurity*
4 *threat’ does not include any action that solely*
5 *involves a violation of a consumer term of service*
6 *or a consumer licensing agreement.*

7 “(10) *DEFENSIVE MEASURE.*—

8 “(A) *IN GENERAL.*—*Except as provided in*
9 *subparagraph (B), the term ‘defensive measure’*
10 *means an action, device, procedure, signature,*
11 *technique, or other measure applied to an infor-*
12 *mation system or information that is stored on,*
13 *processed by, or transiting an information sys-*
14 *tem that detects, prevents, or mitigates a known*
15 *or suspected cybersecurity threat or security vul-*
16 *nerability.*

17 “(B) *EXCLUSION.*—*The term ‘defensive*
18 *measure’ does not include a measure that de-*
19 *stroys, renders unusable, provides unauthorized*
20 *access to, or substantially harms an information*
21 *system or information stored on, processed by, or*
22 *transiting such information system not owned*
23 *by—*

24 “(i) *the entity operating the measure;*

25 *or*

1 “(ii) another entity or Federal entity
2 that is authorized to provide consent and
3 has provided consent to that private entity
4 for operation of such measure.

5 “(11) *HOMELAND SECURITY ENTERPRISE*.—The
6 term ‘Homeland Security Enterprise’ means relevant
7 governmental and nongovernmental entities involved
8 in homeland security, including Federal, State, local,
9 and tribal government officials, private sector rep-
10 resentatives, academics, and other policy experts.

11 “(12) *INCIDENT*.—The term ‘incident’ means an
12 occurrence that actually or imminently jeopardizes,
13 without lawful authority, the integrity, confiden-
14 tiality, or availability of information on an informa-
15 tion system, or actually or imminently jeopardizes,
16 without lawful authority, an information system.

17 “(13) *INFORMATION SHARING AND ANALYSIS OR-*
18 *GANIZATION*.—The term ‘Information Sharing and
19 Analysis Organization’ means any formal or infor-
20 mal entity or collaboration created or employed by
21 public or private sector organizations, for purposes
22 of—

23 “(A) gathering and analyzing critical infra-
24 structure information, including information re-
25 lated to cybersecurity risks and incidents, in

1 *order to better understand security problems and*
2 *interdependencies related to critical infrastruc-*
3 *ture, including cybersecurity risks and incidents,*
4 *and protected systems, so as to ensure the avail-*
5 *ability, integrity, and reliability thereof;*

6 “(B) *communicating or disclosing critical*
7 *infrastructure information, including cybersecu-*
8 *rity risks and incidents, to help prevent, detect,*
9 *mitigate, or recover from the effects of a inter-*
10 *ference, compromise, or a incapacitation problem*
11 *related to critical infrastructure, including cy-*
12 *bersecurity risks and incidents, or protected sys-*
13 *tems; and*

14 “(C) *voluntarily disseminating critical in-*
15 *frastructure information, including cybersecurity*
16 *risks and incidents, to its members, State, local,*
17 *and Federal Governments, or any other entities*
18 *that may be of assistance in carrying out the*
19 *purposes specified in subparagraphs (A) and*
20 *(B).*

21 “(14) *INFORMATION SYSTEM.*—*The term ‘infor-*
22 *mation system’ has the meaning given the term in*
23 *section 3502 of title 44, United States Code.*

24 “(15) *INTELLIGENCE COMMUNITY.*—*The term*
25 *‘intelligence community’ has the meaning given the*

1 *term in section 3(4) of the National Security Act of*
2 *1947 (50 U.S.C. 3003(4)).*

3 “(16) *MONITOR.*—*The term ‘monitor’ means to*
4 *acquire, identify, or scan, or to possess, information*
5 *that is stored on, processed by, or transiting an infor-*
6 *mation system.*

7 “(17) *NATIONAL CYBERSECURITY ASSET RE-*
8 *SPONSE ACTIVITIES.*—*The term ‘national cybersecu-*
9 *rity asset response activities’ means—*

10 “(A) *furnishing cybersecurity technical as-*
11 *sistance to entities affected by cybersecurity risks*
12 *to protect assets, mitigate vulnerabilities, and re-*
13 *duce impacts of cyber incidents;*

14 “(B) *identifying other entities that may be*
15 *at risk of an incident and assessing risk to the*
16 *same or similar vulnerabilities;*

17 “(C) *assessing potential cybersecurity risks*
18 *to a sector or region, including potential cas-*
19 *cading effects, and developing courses of action to*
20 *mitigate such risks;*

21 “(D) *facilitating information sharing and*
22 *operational coordination with threat response;*
23 *and*

24 “(E) *providing guidance on how best to uti-*
25 *lize Federal resources and capabilities in a time-*

1 *ly, effective manner to speed recovery from cyber-*
2 *security risks.*

3 “(18) *NATIONAL SECURITY SYSTEM.*—*The term*
4 *‘national security system’ has the meaning given the*
5 *term in section 11103 of title 40, United States Code.*

6 “(19) *SECTOR RISK MANAGEMENT AGENCY.*—*The*
7 *term ‘Sector Risk Management Agency’ means a Fed-*
8 *eral department or agency, designated by law or Pres-*
9 *idential directive, with responsibility for providing*
10 *institutional knowledge and specialized expertise of a*
11 *sector, as well as leading, facilitating, or supporting*
12 *programs and associated activities of its designated*
13 *critical infrastructure sector in the all hazards envi-*
14 *ronment in coordination with the Department.*

15 “(20) *SECURITY CONTROL.*—*The term ‘security*
16 *control’ means the management, operational, and*
17 *technical controls used to protect against an unau-*
18 *thorized effort to adversely affect the confidentiality,*
19 *integrity, and availability of an information system*
20 *or its information.*

21 “(21) *SECURITY VULNERABILITY.*—*The term ‘se-*
22 *curity vulnerability’ means any attribute of hard-*
23 *ware, software, process, or procedure that could enable*
24 *or facilitate the defeat of a security control.*

1 “(22) *SHARING*.—The term ‘sharing’ (including
2 all conjugations thereof) means providing, receiving,
3 and disseminating (including all conjugations of each
4 such terms).”.

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

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

9 **“SEC. 2201. DEFINITION.**

10 *“In this subtitle, the term ‘Cybersecurity Advisory*
11 *Committee’ means the advisory committee established under*
12 *section 2219(a).”;*

13 (2) *in section 2202—*

14 (A) *in subsection (a)(1), by striking “(in*
15 *this subtitle referred to as the Agency)”;*

16 (B) *in subsection (f)—*

17 (i) *in paragraph (1), by inserting “Ex-*
18 *ecutive” before “Assistant Director”;* and

19 (ii) *in paragraph (2), by inserting*
20 *“Executive” before “Assistant Director”;*

21 (3) *in section 2203(a)(2), by striking “as the*
22 *‘Assistant Director’” and inserting “as the ‘Executive*
23 *Assistant Director’”;*

1 (4) in section 2204(a)(2), by striking “as the
2 ‘Assistant Director’” and inserting “as the ‘Executive
3 Assistant Director’”;

4 (5) in section 2209—

5 (A) by striking subsection (a);

6 (B) by redesignating subsections (b) through
7 subsection (o) as subsections (a) through (n), re-
8 spectively;

9 (C) in subsection (c)(1)—

10 (i) in subparagraph (A)(iii), as so re-
11 designated, by striking “, as that term is
12 defined under section 3(4) of the National
13 Security Act of 1947 (50 U.S.C. 3003(4))”;
14 and

15 (ii) in subparagraph (B)(ii), by strik-
16 ing “information sharing and analysis or-
17 ganizations” and inserting “Information
18 Sharing and Analysis Organizations”;

19 (D) in subsection (d), as so redesignated—

20 (i) in the matter preceding paragraph
21 (1), by striking “subsection (c)” and insert-
22 ing “subsection (b)”; and

23 (ii) in paragraph (1)(E)(ii)(II), by
24 striking “information sharing and analysis

1 *organizations” and inserting “Information*
2 *Sharing and Analysis Organizations”;*

3 *(E) in subsection (j), as so redesignated, by*
4 *striking “subsection (c)(8)” and inserting “sub-*
5 *section (b)(8)”;* *and*

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

7 *(i) in paragraph (2)(A), by striking*
8 *“subsection (c)(12)” and inserting “sub-*
9 *section (b)(12)”;* *and*

10 *(ii) in paragraph (3)(B)(i), by striking*
11 *“subsection (c)(12)” and inserting “sub-*
12 *section (b)(12)”;*

13 *(6) in section 2210—*

14 *(A) by striking subsection (a);*

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

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

18 *(i) by striking “information sharing*
19 *and analysis organizations (as defined in*
20 *section 2222(5))” and inserting “Informa-*
21 *tion Sharing and Analysis Organizations”;*

22 *and*

23 *(ii) by striking “(as defined in section*
24 *2209)”;* *and*

1 (D) in subsection (c), as so redesignated, by
2 striking “subsection (c)” and inserting “sub-
3 section (b)”;

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

5 (8) in section 2212, by striking “information
6 sharing and analysis organizations (as defined in sec-
7 tion 2222(5))” and inserting “Information Sharing
8 and Analysis Organizations”;

9 (9) in section 2213—

10 (A) by striking subsection (a);

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

13 (C) in subsection (b), as so redesignated, by
14 striking “subsection (b)” each place it appears
15 and inserting “subsection (a)”;

16 (D) in subsection (c), as so redesignated, in
17 the matter preceding paragraph (1), by striking
18 “subsection (b)” and inserting “subsection (a)”;

19 and

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

21 (i) in paragraph (1)—

22 (I) in the matter preceding sub-
23 paragraph (A), by striking “subsection
24 (c)(2)” and inserting “subsection
25 (b)(2)”;

1 (II) in subparagraph (A), by
2 striking “subsection (c)(1)” and insert-
3 ing “subsection (b)(1)”; and

4 (III) in subparagraph (B), by
5 striking “subsection (c)(2)” and insert-
6 ing “subsection (b)(2)”; and

7 (ii) in paragraph (2), by striking
8 “subsection (c)(2)” and inserting “sub-
9 section (b)(2)”; and

10 (10) in section 2216, as so redesignated—

11 (A) in subsection (d)(2), by striking “infor-
12 mation sharing and analysis organizations” and
13 inserting “Information Sharing and Analysis
14 Organizations”; and

15 (B) by striking subsection (f) and inserting
16 the following:

17 “(f) *CYBER DEFENSE OPERATION DEFINED.*—In this
18 section, the term ‘cyber defense operation’ means the use of
19 a defensive measure.”;

20 (11) in section 2218(c)(4)(A), as so redesignated,
21 by striking “information sharing and analysis orga-
22 nizations” and inserting “Information Sharing and
23 Analysis Organizations”; and

24 (12) in section 2222—

1 (A) by striking paragraphs (3), (5), and
2 (8);

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

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

7 (c) *TABLE OF CONTENTS AMENDMENTS.*—The table of
8 contents in section 1(b) of the Homeland Security Act of
9 2002 (Public Law 107–296; 116 Stat. 2135) is amended—

10 (1) by inserting before the item relating to sub-
11 title A of title XXII the following:

“Sec. 2200. Definitions.”;

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

“Sec. 2201. Definition.”; and

14 (3) by striking the item relating to section 2214
15 and all that follows through the item relating to sec-
16 tion 2217 and inserting the following:

“Sec. 2214. National Asset Database.

“Sec. 2215. Duties and authorities relating to .gov internet domain.

“Sec. 2216. Joint Cyber Planning Office.

“Sec. 2217. Cybersecurity State Coordinator.

“Sec. 2218. Sector Risk Management Agencies.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity Education and Training Programs.”.

17 (d) *CYBERSECURITY ACT OF 2015 DEFINITIONS.*—Sec-
18 tion 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)
19 is amended—

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

3 “(4) *CYBERSECURITY PURPOSE.—The term ‘cy-*
4 *bersecurity purpose’ has the meaning given the term*
5 *in section 2200 of the Homeland Security Act of*
6 *2002.*

7 “(5) *CYBERSECURITY THREAT.—The term ‘cy-*
8 *bersecurity threat’ has the meaning given the term in*
9 *section 2200 of the Homeland Security Act of 2002.*

10 “(6) *CYBER THREAT INDICATOR.—The term*
11 *‘cyber threat indicator’ has the meaning given the*
12 *term in section 2200 of the Homeland Security Act*
13 *of 2002.*

14 “(7) *DEFENSIVE MEASURE.—The term ‘defensive*
15 *measure’ has the meaning given the term in section*
16 *2200 of the Homeland Security Act of 2002.’;*

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

19 “(13) *MONITOR.— The term ‘monitor’ has the*
20 *meaning given the term in section 2200 of the Home-*
21 *land Security Act of 2002.’; and*

22 (3) *by striking paragraphs (16) and (17) and*
23 *inserting the following:*

1 “(16) *SECURITY CONTROL*.—*The term ‘security*
 2 *control’ has the meaning given the term in section*
 3 *2200 of the Homeland Security Act of 2002.*

4 “(17) *SECURITY VULNERABILITY*.—*The term ‘se-*
 5 *curity vulnerability’ has the meaning given the term*
 6 *in section 2200 of the Homeland Security Act of*
 7 *2002.’.*”

8 **SEC. 4. ADDITIONAL TECHNICAL AND CONFORMING**
 9 **AMENDMENTS.**

10 (a) *FEDERAL CYBERSECURITY ENHANCEMENT ACT OF*
 11 *2015*.—*The Federal Cybersecurity Enhancement Act of*
 12 *2015 (6 U.S.C. 1521 et seq.) is amended—*

13 (1) *in section 222 (6 U.S.C. 1521)—*

14 (A) *in paragraph (2), by striking “section*
 15 *2210” and inserting “section 2200”; and*

16 (B) *in paragraph (4), by striking “section*
 17 *2209” and inserting “section 2200”;*

18 (2) *in section 223(b) (6 U.S.C. 151 note), by*
 19 *striking “section 2213(b)(1)” each place it appears*
 20 *and inserting “section 2213(a)(1)”;*

21 (3) *in section 226 (6 U.S.C. 1524)—*

22 (A) *in subsection (a)—*

23 (i) *in paragraph (1), by striking “sec-*
 24 *tion 2213” and inserting “section 2200”;*

1 (ii) in paragraph (2), by striking “sec-
2 tion 102” and inserting “section 2200 of the
3 Homeland Security Act of 2002”;

4 (iii) in paragraph (4), by striking
5 “section 2210(b)(1)” and inserting “section
6 2210(a)(1)”; and

7 (iv) in paragraph (5), by striking “sec-
8 tion 2213(b)” and inserting “section
9 2213(a)”; and

10 (B) in subsection (c)(1)(A)(vi), by striking
11 “section 2213(c)(5)” and inserting “section
12 2213(b)(5)”; and

13 (4) in section 227(b) (6 U.S.C. 1525(b)), by
14 striking “section 2213(d)(2)” and inserting “section
15 2213(c)(2)”.

16 (b) *PUBLIC HEALTH SERVICE ACT.*—Section
17 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C.
18 300hh–10(b)(4)(D)) is amended by striking “section 228(c)
19 of the Homeland Security Act of 2002 (6 U.S.C. 149(c))”
20 and inserting “section 2210(b) of the Homeland Security
21 Act of 2002 (6 U.S.C. 660(b))”.

22 (c) *WILLIAM M. (MAC) THORNBERRY NATIONAL DE-*
23 *FENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.*—Sec-
24 tion 9002 of the William M. (Mac) Thornberry National

1 *Defense Authorization Act for Fiscal Year 2021 (6 U.S.C.*
2 *652a) is amended—*

3 *(1) in subsection (a)—*

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

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

10 *“(7) SECTOR RISK MANAGEMENT AGENCY.—The*
11 *term ‘Sector Risk Management Agency’ has the mean-*
12 *ing given the term in section 2200 of the Homeland*
13 *Security Act of 2002.”;*

14 *(2) in subsection (c)(3)(B), by striking “section*
15 *2201(5)” and inserting “section 2200”; and*

16 *(3) in subsection (d)—*

17 *(A) by striking “section 2215” and insert-*
18 *ing “2218”; and*

19 *(B) by striking “, as added by this section”.*

20 *(d) NATIONAL SECURITY ACT OF 1947.—Section 113B*
21 *of the National Security Act of 1947 (50 U.S.C.*
22 *3049a(b)(4)) is amended by striking section “226 of the*
23 *Homeland Security Act of 2002 (6 U.S.C. 147)” and insert-*
24 *ing “section 2208 of the Homeland Security Act of 2002*
25 *(6 U.S.C. 658)”.*

1 (e) *IoT CYBERSECURITY IMPROVEMENT ACT OF*
2 *2020.—Section 5(b)(3) of the IoT Cybersecurity Improve-*
3 *ment Act of 2020 (15 U.S.C. 278g–3c) is amended by strik-*
4 *ing “section 2209(m) of the Homeland Security Act of 2002*
5 *(6 U.S.C. 659(m))” and inserting “section 2209(l) of the*
6 *Homeland Security Act of 2002 (6 U.S.C. 659(l))”.*

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

10 (g) *TITLE 46.—Section 70101(2) of title 46, United*
11 *States Code, is amended by striking “section 227 of the*
12 *Homeland Security Act of 2002 (6 U.S.C. 148)” and insert-*
13 *ing “section 2200 of the Homeland Security Act of 2002”.*

Calendar No. 632

117TH CONGRESS
2^D SESSION

S. 2540

[Report No. 117-248]

A BILL

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

DECEMBER 13, 2022

Reported with an amendment