

117TH CONGRESS
1ST SESSION

S. 2540

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 and Mr. PETERS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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”.

6 **SEC. 2. REDESIGNATIONS.**

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

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

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

3 (3) by redesignating section 2217 (6 U.S.C.
4 665f) as section 2219;

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

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

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

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

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

19 (1) in section 320(d)(3)(C) (6 U.S.C.
20 195f(d)(3)(C)) by striking “section 2201” and in-
21 serting “section 2200”;

22 (2) in section 846(1) (6 U.S.C. 417(1)), by
23 striking “section 2209” and inserting “section
24 2208”;

1 (3) in section 1801(c)(16) (6 U.S.C.
2 571(c)(16)) by striking “section 2202(e)(7)” and in-
3 serting “section 2201(c)(7)”;

4 (4) in section 2001(4)(A)(iii)(II) (6 U.S.C.
5 601(4)(A)(iii)(II)), by striking “section 2214(a)(2)”
6 and inserting “section 2213(a)(2)”;

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

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

11 (A) in subsection (c)—

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

15 (ii) by redesignating the second and
16 third paragraphs (12) as paragraphs (13)
17 and (14), respectively; and

18 (iii) in paragraph (13), as so redesign-
19 ated, by striking “section 2215” and in-
20 serting “section 2214”; and

21 (B) in subsection (e)(2), by striking “sec-
22 tions 2203(b) and 2204(b)” and inserting “sec-
23 tions 2202(b) and 2203(b)”;

1 (7) in section 2202(b)(3), as so redesignated,
 2 by striking “section 2202(c)(7)” and inserting “sec-
 3 tion 2201(c)(7)”;

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

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

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

13 (11) in section 2217(c)(4)(A), by striking “sec-
 14 tion 2209” and inserting “section 2208”.

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

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

“Sec. 2200. Definitions.”;

20 and

21 (2) by striking the items relating to sections
 22 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

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

1 **“SEC. 2200. DEFINITIONS.**

2 “Except as otherwise specifically provided, in this
3 title:

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

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

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

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

16 “(A) the Committee on Homeland Security
17 and Governmental Affairs of the Senate; and

18 “(B) the Committee on Homeland Security
19 of the House of Representatives.

20 “(5) CRITICAL INFRASTRUCTURE INFORMA-
21 TION.—The term ‘critical infrastructure information’
22 means information not customarily in the public do-
23 main and related to the security of critical infra-
24 structure or protected systems—

25 “(A) actual, potential, or threatened inter-
26 ference with, attack on, compromise of, or inca-

1 pacitation of critical infrastructure or protected
2 systems by either physical or computer-based
3 attack or other similar conduct (including the
4 misuse of or unauthorized access to all types of
5 communications and data transmission systems)
6 that violates Federal, State, or local law, harms
7 interstate commerce of the United States, or
8 threatens public health or safety;

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

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

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

1 “(A) malicious reconnaissance, including
2 anomalous patterns of communications that ap-
3 pear to be transmitted for the purpose of gath-
4 ering technical information related to a cyberse-
5 curity threat or security vulnerability;

6 “(B) a method of defeating a security con-
7 trol or exploitation of a security vulnerability;

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

11 “(D) a method of causing a user with le-
12 gitimate access to an information system or in-
13 formation that is stored on, processed by, or
14 transiting an information system to unwittingly
15 enable the defeat of a security control or exploi-
16 tation of a security vulnerability;

17 “(E) malicious cyber command and con-
18 trol;

19 “(F) the actual or potential harm caused
20 by an incident, including a description of the in-
21 formation exfiltrated as a result of a particular
22 cybersecurity threat;

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

1 “(H) any combination thereof.

2 “(7) CYBERSECURITY PURPOSE.—The term ‘cybersecurity purpose’ means the purpose of protecting
3 an information system or information that is stored
4 on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability.
5
6
7

8 “(8) CYBERSECURITY RISK.—The term ‘cybersecurity risk’—
9

10 “(A) means threats to and vulnerabilities
11 of information or information systems and any
12 related consequences caused by or resulting
13 from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction
14 of such information or information systems, including such related consequences
15 caused by an act of terrorism; and
16
17

18 “(B) does not include any action that solely involves a violation of a consumer term of
19 service or a consumer licensing agreement.
20

21 “(9) CYBERSECURITY THREAT.—

22 “(A) IN GENERAL.—Except as provided in
23 subparagraph (B), the term ‘cybersecurity
24 threat’ means an action, not protected by the
25 First Amendment to the Constitution of the

1 United States, on or through an information
2 system that may result in an unauthorized ef-
3 fort to adversely impact the security, avail-
4 ability, confidentiality, or integrity of an infor-
5 mation system or information that is stored on,
6 processed by, or transiting an information sys-
7 tem.

8 “(B) EXCLUSION.—The term ‘cybersecu-
9 rity threat’ does not include any action that
10 solely involves a violation of a consumer term of
11 service or a consumer licensing agreement.

12 “(10) DEFENSIVE MEASURE.—

13 “(A) IN GENERAL.—Except as provided in
14 subparagraph (B), the term ‘defensive measure’
15 means an action, device, procedure, signature,
16 technique, or other measure applied to an infor-
17 mation system or information that is stored on,
18 processed by, or transiting an information sys-
19 tem that detects, prevents, or mitigates a
20 known or suspected cybersecurity threat or se-
21 curity vulnerability.

22 “(B) EXCLUSION.—The term ‘defensive
23 measure’ does not include a measure that de-
24 stroys, renders unusable, provides unauthorized
25 access to, or substantially harms an information

1 system or information stored on, processed by,
2 or transiting such information system not
3 owned by—

4 “(i) the entity operating the measure;

5 or

6 “(ii) another entity or Federal entity
7 that is authorized to provide consent and
8 has provided consent to that private entity
9 for operation of such measure.

10 “(11) HOMELAND SECURITY ENTERPRISE.—

11 The term ‘Homeland Security Enterprise’ means rel-
12 evant governmental and nongovernmental entities in-
13 volved in homeland security, including Federal,
14 State, local, and tribal government officials, private
15 sector representatives, academics, and other policy
16 experts.

17 “(12) INCIDENT.—The term ‘incident’ means
18 an occurrence that actually or imminently jeopard-
19 izes, without lawful authority, the integrity, con-
20 fidentiality, or availability of information on an in-
21 formation system, or actually or imminently jeopard-
22 izes, without lawful authority, an information sys-
23 tem.

24 “(13) INFORMATION SHARING AND ANALYSIS
25 ORGANIZATION.—The term ‘Information Sharing

1 and Analysis Organization’ means any formal or in-
2 formal entity or collaboration created or employed by
3 public or private sector organizations, for purposes
4 of—

5 “(A) gathering and analyzing critical infra-
6 structure information, including information re-
7 lated to cybersecurity risks and incidents, in
8 order to better understand security problems
9 and interdependencies related to critical infra-
10 structure, including cybersecurity risks and in-
11 cidents, and protected systems, so as to ensure
12 the availability, integrity, and reliability thereof;

13 “(B) communicating or disclosing critical
14 infrastructure information, including cybersecu-
15 rity risks and incidents, to help prevent, detect,
16 mitigate, or recover from the effects of a inter-
17 ference, compromise, or a incapacitation prob-
18 lem related to critical infrastructure, including
19 cybersecurity risks and incidents, or protected
20 systems; and

21 “(C) voluntarily disseminating critical in-
22 frastructure information, including cybersecu-
23 rity risks and incidents, to its members, State,
24 local, and Federal Governments, or any other
25 entities that may be of assistance in carrying

1 out the purposes specified in subparagraphs (A)
2 and (B).

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

6 “(15) INTELLIGENCE COMMUNITY.—The term
7 ‘intelligence community’ has the meaning given the
8 term in section 3(4) of the National Security Act of
9 1947 (50 U.S.C. 3003(4)).

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

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

17 “(A) furnishing cybersecurity technical as-
18 sistance to entities affected by cybersecurity
19 risks to protect assets, mitigate vulnerabilities,
20 and reduce impacts of cyber incidents;

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

24 “(C) assessing potential cybersecurity risks
25 to a sector or region, including potential cas-

1 cading effects, and developing courses of action
2 to mitigate such risks;

3 “(D) facilitating information sharing and
4 operational coordination with threat response;
5 and

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

10 “(18) NATIONAL SECURITY SYSTEM.—The term
11 ‘national security system’ has the meaning given the
12 term in section 11103 of title 40, United States
13 Code.

14 “(19) SECTOR RISK MANAGEMENT AGENCY.—
15 The term ‘Sector Risk Management Agency’ means
16 a Federal department or agency, designated by law
17 or Presidential directive, with responsibility for pro-
18 viding institutional knowledge and specialized exper-
19 tise of a sector, as well as leading, facilitating, or
20 supporting programs and associated activities of its
21 designated critical infrastructure sector in the all
22 hazards environment in coordination with the De-
23 partment.

24 “(20) SECURITY VULNERABILITY.—The term
25 ‘security vulnerability’ means any attribute of hard-

1 ware, software, process, or procedure that could en-
2 able or facilitate the defeat of a security control.

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

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

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

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

13 (B) in subsection (f)—

14 (i) in paragraph (1), by inserting
15 “Executive” before “Assistant Director”;

16 and

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

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

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

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

1 (A) by striking subsection (a);

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

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

9 (D) in subsection (d), as so redesignated,
10 in the matter preceding paragraph (1), by strik-
11 ing “subsection (c)” and inserting “subsection
12 (b)”;

13 (E) in subsection (j), as so redesignated,
14 by striking “subsection (c)(8)” and inserting
15 “subsection (b)(8)”; and

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

17 (i) in paragraph (2)(A), by striking
18 “subsection (c)(12)” and inserting “sub-
19 section (b)(12)”; and

20 (ii) in paragraph (3)(B)(i), by striking
21 “subsection (c)(12)” and inserting “sub-
22 section (b)(12)”;

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

24 (A) by striking subsection (a);

1 (B) by redesignating subsections (b)
2 through (d) as subsections (a) through (c), re-
3 spectively;

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

5 (i) by striking “information sharing
6 and analysis organizations (as defined in
7 section 2222(5))” and inserting “Informa-
8 tion Sharing and Analysis Organizations”;
9 and

10 (ii) by striking “(as defined in section
11 2209)” and

12 (D) in subsection (c), as so redesignated,
13 by striking “subsection (c)” and inserting “sub-
14 section (b)”;

15 (6) in section 2210, as so redesignated, by
16 striking subsection (h);

17 (7) in section 2211, as so redesignated, by
18 striking “information sharing and analysis organiza-
19 tions (as defined in section 2222(5))” and inserting
20 “Information Sharing and Analysis Organizations”;

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

22 (A) by striking subsection (a);

23 (B) by redesignating subsections (b)
24 through (f) as subsections (a) through (e); re-
25 spectively;

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

4 (D) in subsection (c), as so redesignated,
5 in the matter preceding paragraph (1), by strik-
6 ing “subsection (b)” and inserting “subsection
7 (a)”;

8 (E) in subsection (d), as so redesignated—
9 (i) in paragraph (1)—

10 (I) in the matter preceding sub-
11 paragraph (A), by striking “sub-
12 section (c)(2)” and inserting “sub-
13 section (b)(2)”;

14 (II) in subparagraph (A), by
15 striking “subsection (c)(1)” and in-
16 serting “subsection (b)(1)”;

17 (III) in subparagraph (B), by
18 striking “subsection (c)(2)” and in-
19 serting “subsection (b)(2)”;

20 (ii) in paragraph (2), by striking
21 “subsection (c)(2)” and inserting “sub-
22 section (b)(2)”;

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

24 (A) by striking subsection (a);

1 (B) by redesignating subsections (b)
2 through (h) as subsections (a) through (g), re-
3 spectively;

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

5 (i) in the matter preceding paragraph
6 (1), by striking “subsection (e)” and in-
7 serting “subsection (d)”;

8 (ii) in paragraph (1), by striking
9 “subsection (c)” and inserting “subsection
10 (b)”;

11 (iii) in paragraph (2), by striking
12 “subsection (c)” and inserting “subsection
13 (b)”;

14 (D) in subsection (b)(4), as so redesign-
15 ated—

16 (i) by striking “subsection (e)” and
17 inserting “subsection (d)”;

18 (ii) by striking “subsection (h)” and
19 inserting “subsection (g)”;

20 (E) in subsection (d), as so redesignated,
21 by striking “subsection (b)(1)” each place it ap-
22 pears and inserting “subsection (a)(1)”;

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

24 (i) by striking “subsection (b)” and
25 inserting “subsection (a)”;

1 (ii) by striking “subsection (e)” and
2 inserting “subsection (d)”; and

3 (iii) by striking “subsection (b)(1)”
4 and inserting “subsection (a)(1)”; and

5 (G) in subsection (f), as so redesignated,
6 by striking “subsection (e)” and inserting “sub-
7 section (b)”;

8 (10) in section 2216, as so redesignated, by
9 striking subsection (f) and inserting the following:

10 “(f) CYBER DEFENSE OPERATION DEFINED.—In
11 this section, the term ‘cyber defense operation’ means the
12 use of a defensive measure.”; and

13 (11) in section 2222—

14 (A) by striking paragraphs (3), (5), and
15 (8);

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

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

20 (e) CYBERSECURITY ACT OF 2015 DEFINITIONS.—

21 Section 102 of the Cybersecurity Act of 2015 (6 U.S.C.
22 1501) is amended—

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

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

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

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

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

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

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

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

23 “(17) SECURITY VULNERABILITY.—The term
24 ‘security vulnerability’ has the meaning given the

1 term in section 2200 of the Homeland Security Act
2 of 2002.”.

3 **SEC. 4. ADDITIONAL TECHNICAL AND CONFORMING**
4 **AMENDMENTS.**

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

8 (1) in section 222 (6 U.S.C. 1521)—

9 (A) in paragraph (2), by striking “section
10 2210” and inserting “section 2200”; and

11 (B) in paragraph (4), by striking “section
12 2209” and inserting “section 2200”;

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

16 (3) in section 226—

17 (A) in subsection (a)—

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

20 (ii) in paragraph (4), by striking “sec-
21 tion 2210(b)(1)” and inserting “section
22 2209(a)(1)”; and

23 (iii) in paragraph (5), by striking
24 “section 2213(b)” and inserting “section
25 2212(a)”; and

1 (B) in subsection (c)(1)(A)(vi), by striking
2 “section 2213(c)(5)” and inserting “section
3 2212(b)(5)”; and

4 (4) in section 227 (6 U.S.C. 1525)—

5 (A) in subsection (a), by striking “section
6 2213” and inserting “section 2212”; and

7 (B) in subsection (b), by striking “section
8 2213(d)(2)” and inserting “section
9 2212(c)(2)”.

10 (b) PUBLIC HEALTH SERVICE ACT.—Section
11 2811(b)(4)(D) of the Public Health Service Act (42
12 U.S.C. 300hh–10(b)(4)(D)) is amended by striking “sec-
13 tion 228(c) of the Homeland Security Act of 2002 (6
14 U.S.C. 149(c))” and inserting “section 2209(c) of the
15 Homeland Security Act of 2002”.

16 (c) WILLIAM M. (MAC) THORNBERRY NATIONAL DE-
17 FENSE AUTHORIZATION ACT OF FISCAL YEAR 2021.—
18 Section 9002 of the William M. (Mac) Thornberry Na-
19 tional Defense Authorization Act for Fiscal Year 2021 (6
20 U.S.C. 652a) is amended—

21 (1) in subsection (a)—

22 (A) in paragraph (5), by striking “section
23 2222(5) of the Homeland Security Act of 2002
24 (6 U.S.C. 671(5))” and inserting “section 2200
25 of the Homeland Security Act of 2002”; and

1 (B) in paragraph (7), by striking “given
2 the term” and all that follows and inserting
3 “given the term in section 2200 of the Home-
4 land Security Act of 2002”;

5 (2) in subsection (b)(1)(A), by striking “section
6 2202(c)(4) of the Homeland Security Act (6 U.S.C.
7 652(c)(4))” and inserting “section 2201(c)(4)”;

8 (3) in subsection (c)(3)(B), by striking “section
9 2201(5) of the Homeland Security Act of 2002 (6
10 U.S.C. 651(5))” and inserting “section 2200 of the
11 Homeland Security Act of 2002”; and

12 (4) in subsection (d)—

13 (A) by striking “section 2215” and insert-
14 ing “2217”; and

15 (B) by striking “, as added by this sec-
16 tion”.

17 (d) NATIONAL SECURITY ACT OF 1947.—Section
18 113B of the National Security Act of 1947 (50 U.S.C.
19 3049a(b)(4)) is amended by striking section “226 of the
20 Homeland Security Act of 2002 (6 U.S.C. 147)” and in-
21 serting “section 2207 of the Homeland Security Act of
22 2002”.

23 (e) CYBERSECURITY ACT OF 2015.—Section 404(a)
24 of the Cybersecurity Act of 2015 (6 U.S.C. 1532(a)) is

1 amended by striking “section 2209” and inserting “sec-
2 tion 2208”.

3 (f) IOT CYBERSECURITY IMPROVEMENT ACT OF
4 2020.—Section 5(b)(3) of the IoT Cybersecurity Improve-
5 ment Act of 2020 (15 U.S.C. 278g–3e) is amended by
6 striking “section 2209(m)” and inserting “section
7 2208(l)”.

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

12 (h) TITLE 46.—Section 70101(2) of title 46, United
13 States Code, is amended by striking “section 227 of the
14 Homeland Security Act of 2002 (6 U.S.C. 148)” and in-
15 serting “section 2200 of the Homeland Security Act of
16 2002”.

○