

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:

1 Strike all after the enacting clause and insert the fol-
2 lowing:

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 redesignating section 2217 (6 U.S.C.
11 665f) as section 2220;

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

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

6 (4) by redesignating the third section 2215 (re-
7 lating to the Cybersecurity State Coordinator) (6
8 U.S.C. 665e) as section 2217; and

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

12 (b) TECHNICAL AND CONFORMING AMENDMENTS.—
13 Section 2202(c) of the Homeland Security Act of 2002
14 (6 U.S.C. 652(c)) is amended—

15 (1) in the first paragraph (12), by striking
16 “section 2215” and inserting “section 2217”; and

17 (2) by redesignating the second and third para-
18 graphs (12) as paragraphs (13) and (14), respec-
19 tively.

20 (c) ADDITIONAL TECHNICAL AMENDMENT.—

21 (1) AMENDMENT.—Section 904(b)(1) of the
22 DOTGOV Act of 2020 (title IX of division U of
23 Public Law 116–260) is amended, in the matter pre-
24 ceding subparagraph (A), by striking “Homeland

1 Security Act” and inserting “Homeland Security Act
2 of 2002”.

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

7 **SEC. 3. CONSOLIDATION OF DEFINITIONS.**

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

11 **“SEC. 2200. DEFINITIONS.**

12 “Except as otherwise specifically provided, in this
13 title:

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

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

19 “(3) AGENCY INFORMATION SYSTEM.—The
20 term ‘agency information system’ means an informa-
21 tion system used or operated by an agency or by an-
22 other entity on behalf of an agency.

23 “(4) APPROPRIATE CONGRESSIONAL COMMIT-
24 TEES.—The term ‘appropriate congressional com-
25 mittees’ means—

1 “(A) the Committee on Homeland Security
2 and Governmental Affairs of the Senate; and

3 “(B) the Committee on Homeland Security
4 of the House of Representatives.

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

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

20 “(B) the ability of any critical infrastruc-
21 ture or protected system to resist such inter-
22 ference, compromise, or incapacitation, includ-
23 ing any planned or past assessment, projection,
24 or estimate of the vulnerability of critical infra-
25 structure or a protected system, including secu-

1 rity testing, risk evaluation thereto, risk man-
2 agement planning, or risk audit; or

3 “(C) any planned or past operational prob-
4 lem or solution regarding critical infrastructure
5 or protected systems, including repair, recovery,
6 reconstruction, insurance, or continuity, to the
7 extent it is related to such interference, com-
8 promise, or incapacitation.

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

12 “(A) malicious reconnaissance, including
13 anomalous patterns of communications that ap-
14 pear to be transmitted for the purpose of gath-
15 ering technical information related to a cyberse-
16 curity threat or security vulnerability;

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

19 “(C) a security vulnerability, including
20 anomalous activity that appears to indicate the
21 existence of a security vulnerability;

22 “(D) a method of causing a user with le-
23 gitimate access to an information system or in-
24 formation that is stored on, processed by, or
25 transiting an information system to unwittingly

1 enable the defeat of a security control or exploi-
2 tation of a security vulnerability;

3 “(E) malicious cyber command and con-
4 trol;

5 “(F) the actual or potential harm caused
6 by an incident, including a description of the in-
7 formation exfiltrated as a result of a particular
8 cybersecurity threat;

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

12 “(H) any combination thereof.

13 “(7) CYBERSECURITY PURPOSE.—The term ‘cy-
14 bersecurity purpose’ means the purpose of protecting
15 an information system or information that is stored
16 on, processed by, or transiting an information sys-
17 tem from a cybersecurity threat or security vulner-
18 ability.

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

21 “(A) means threats to and vulnerabilities
22 of information or information systems and any
23 related consequences caused by or resulting
24 from unauthorized access, use, disclosure, deg-
25 radation, disruption, modification, or destruc-

1 tion of such information or information sys-
2 tems, including such related consequences
3 caused by an act of terrorism; and

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

7 “(9) CYBERSECURITY THREAT.—

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

19 “(B) EXCLUSION.—The term ‘cybersecu-
20 rity threat’ does not include any action that
21 solely involves a violation of a consumer term of
22 service or a consumer licensing agreement.

23 “(10) DEFENSIVE MEASURE.—

24 “(A) IN GENERAL.—Except as provided in
25 subparagraph (B), the term ‘defensive measure’

1 means an action, device, procedure, signature,
2 technique, or other measure applied to an infor-
3 mation system or information that is stored on,
4 processed by, or transiting an information sys-
5 tem that detects, prevents, or mitigates a
6 known or suspected cybersecurity threat or se-
7 curity vulnerability.

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

15 “(i) the entity operating the measure;

16 or

17 “(ii) another entity or Federal entity
18 that is authorized to provide consent and
19 has provided consent to that private entity
20 for operation of such measure.

21 “(11) HOMELAND SECURITY ENTERPRISE.—

22 The term ‘Homeland Security Enterprise’ means rel-
23 evant governmental and nongovernmental entities in-
24 volved in homeland security, including Federal,
25 State, local, and tribal government officials, private

1 sector representatives, academics, and other policy
2 experts.

3 “(12) INCIDENT.—The term ‘incident’ means
4 an occurrence that actually or imminently jeopard-
5 izes, without lawful authority, the integrity, con-
6 fidentiality, or availability of information on an in-
7 formation system, or actually or imminently jeopard-
8 izes, without lawful authority, an information sys-
9 tem.

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

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

24 “(B) communicating or disclosing critical
25 infrastructure information, including cybersecu-

1 rity risks and incidents, to help prevent, detect,
2 mitigate, or recover from the effects of a inter-
3 ference, compromise, or a incapacitation prob-
4 lem related to critical infrastructure, including
5 cybersecurity risks and incidents, or protected
6 systems; and

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

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

17 “(15) INTELLIGENCE COMMUNITY.—The term
18 ‘intelligence community’ has the meaning given the
19 term in section 3(4) of the National Security Act of
20 1947 (50 U.S.C. 3003(4)).

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

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

4 “(A) furnishing cybersecurity technical as-
5 sistance to entities affected by cybersecurity
6 risks to protect assets, mitigate vulnerabilities,
7 and reduce impacts of cyber incidents;

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

11 “(C) assessing potential cybersecurity risks
12 to a sector or region, including potential cas-
13 cading effects, and developing courses of action
14 to mitigate such risks;

15 “(D) facilitating information sharing and
16 operational coordination with threat response;
17 and

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

22 “(18) NATIONAL SECURITY SYSTEM.—The term
23 ‘national security system’ has the meaning given the
24 term in section 11103 of title 40, United States
25 Code.

1 “(19) SECTOR RISK MANAGEMENT AGENCY.—
2 The term ‘Sector Risk Management Agency’ means
3 a Federal department or agency, designated by law
4 or Presidential directive, with responsibility for pro-
5 viding institutional knowledge and specialized exper-
6 tise of a sector, as well as leading, facilitating, or
7 supporting programs and associated activities of its
8 designated critical infrastructure sector in the all
9 hazards environment in coordination with the De-
10 partment.

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

15 “(21) SHARING.—The term ‘sharing’ (including
16 all conjugations thereof) means providing, receiving,
17 and disseminating (including all conjugations of each
18 such terms).”.

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

22 (1) by amending section 2201 to read as fol-
23 lows:

1 **“SEC. 2201. DEFINITION.**

2 “In this subtitle, the term ‘Cybersecurity Advisory
3 Committee’ means the advisory committee established
4 under section 2219(a).”;

5 (2) in section 2202—

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

8 (B) in subsection (f)—

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

11 and

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

14 (3) in section 2203(a)(2), by striking “as the
15 ‘Assistant Director’” and inserting “as the ‘Execu-
16 tive Assistant Director’”;

17 (4) in section 2204(a)(2), by striking “as the
18 ‘Assistant Director’” and inserting “as the ‘Execu-
19 tive Assistant Director’”;

20 (5) in section 2209—

21 (A) by striking subsection (a);

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

25 (C) in subsection (c)(1)(A)(iii), as so re-
26 designated, by striking “, as that term is de-

1 fined under section 3(4) of the National Secu-
2 rity Act of 1947 (50 U.S.C. 3003(4))”;

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

7 (E) in subsection (j), as so redesignated,
8 by striking “subsection (e)(8)” and inserting
9 “subsection (b)(8)”;

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

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

14 (ii) in paragraph (3)(B)(i), by striking
15 “subsection (e)(12)” and inserting “sub-
16 section (b)(12)”;

17 (6) in section 2210—

18 (A) by striking subsection (a);

19 (B) by redesignating subsections (b)
20 through (d) as subsections (a) through (c), re-
21 spectively;

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

23 (i) by striking “information sharing
24 and analysis organizations (as defined in
25 section 2222(5))” and inserting “Informa-

1 tion Sharing and Analysis Organizations”;

2 and

3 (ii) by striking “(as defined in section

4 2209)”; and

5 (D) in subsection (c), as so redesignated,

6 by striking “subsection (c)” and inserting “sub-

7 section (b)”;

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

9 (8) in section 2212, by striking “information

10 sharing and analysis organizations (as defined in

11 section 2222(5))” and inserting “Information Shar-

12 ing and Analysis Organizations”;

13 (9) in section 2213—

14 (A) by striking subsection (a);

15 (B) by redesignating subsections (b)

16 through (f) as subsections (a) through (e); re-

17 spectively;

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

19 by striking “subsection (b)” each place it ap-

20 pears and inserting “subsection (a)”;

21 (D) in subsection (c), as so redesignated,

22 in the matter preceding paragraph (1), by strik-

23 ing “subsection (b)” and inserting “subsection

24 (a)”;

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

1 (i) in paragraph (1)—

2 (I) in the matter preceding sub-
3 paragraph (A), by striking “sub-
4 section (c)(2)” and inserting “sub-
5 section (b)(2)”;

6 (II) in subparagraph (A), by
7 striking “subsection (c)(1)” and in-
8 serting “subsection (b)(1)”; and

9 (III) in subparagraph (B), by
10 striking “subsection (c)(2)” and in-
11 serting “subsection (b)(2)”; and

12 (ii) in paragraph (2), by striking
13 “subsection (c)(2)” and inserting “sub-
14 section (b)(2)”;

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

16 (A) by striking subsection (a);

17 (B) by redesignating subsections (b)
18 through (h) as subsections (a) through (g), re-
19 spectively;

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

21 (i) in the matter preceding paragraph
22 (1), by striking “subsection (e)” and in-
23 serting “subsection (d)”;

1 (ii) in paragraph (1), by striking
2 “subsection (c)” and inserting “subsection
3 (b)”;

4 (iii) in paragraph (2), by striking
5 “subsection (c)” and inserting “subsection
6 (b)”;

7 (D) in subsection (b)(4), as so redesign-
8 nated—

9 (i) by striking “subsection (e)” and
10 inserting “subsection (d)”;

11 (ii) by striking “subsection (h)” and
12 inserting “subsection (g)”;

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

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

17 (i) by striking “subsection (b)” and
18 inserting “subsection (a)”;

19 (ii) by striking “subsection (e)” and
20 inserting “subsection (d)”;

21 (iii) by striking “subsection (b)(1)”
22 and inserting “subsection (a)(1)”;

23 (G) in subsection (f), as so redesignated,
24 by striking “subsection (c)” and inserting “sub-
25 section (b)”;

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

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

6 (12) in section 2222—

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

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

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

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

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

“Sec. 2200. Definitions.”;

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

“Sec. 2201. Definition.”; and

21 (3) by striking the second item relating to sec-
22 tion 2215 and all that follows through the item re-
23 lating to section 2217 and inserting the following:

“Sec. 2216. Cybersecurity State Coordinator.

“Sec. 2217. Joint Cyber Planning Office.

“Sec. 2218. Duties and authorities relating to .gov internet domain.

“Sec. 2219. Cybersecurity Advisory Committee.

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

1 (d) CYBERSECURITY ACT OF 2015 DEFINITIONS.—

2 Section 102 of the Cybersecurity Act of 2015 (6 U.S.C.

3 1501) is amended—

4 (1) by striking paragraphs (4) through (7) and

5 inserting the following:

6 “(4) CYBERSECURITY PURPOSE.—The term ‘cy-

7 bersecurity purpose’ has the meaning given the term

8 in section 2200 of the Homeland Security Act of

9 2002.

10 “(5) CYBERSECURITY THREAT.—The term ‘cy-

11 bersecurity threat’ has the meaning given the term

12 in section 2200 of the Homeland Security Act of

13 2002.

14 “(6) CYBER THREAT INDICATOR.—The term

15 ‘cyber threat indicator’ has the meaning given the

16 term in section 2200 of the Homeland Security Act

17 of 2002.

18 “(7) DEFENSIVE MEASURE.—The term ‘defen-

19 sive measure’ has the meaning given the term in sec-

20 tion 2200 of the Homeland Security Act of 2002.”;

21 (2) by striking paragraph (13) and inserting

22 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 2213(a)(1)”;

23 (3) in section 226—

24 (A) in subsection (a)—

21

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 2210(a)(1)”; and

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

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

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

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

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

1 (1) in subsection (a)—

2 (A) in paragraph (5), by striking “section
3 2222(5) of the Homeland Security Act of 2002
4 (6 U.S.C. 671(5))” and inserting “section 2200
5 of the Homeland Security Act of 2002”; and

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

8 “(7) SECTOR RISK MANAGEMENT AGENCY.—
9 The term ‘Sector Risk Management Agency’ has the
10 meaning given the term in section 2200 of the
11 Homeland Security Act of 2002.”;

12 (2) in subsection (c)(3)(B), by striking “section
13 2201(5) of the Homeland Security Act of 2002 (6
14 U.S.C. 651(5))” and inserting “section 2200 of the
15 Homeland Security Act of 2002”; 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 sec-
20 tion”.

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

1 serting “section 2206 of the Homeland Security Act of
2 2002”.

3 (e) 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 2209(l)”.

8 (f) 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 (g) 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”.