monetary value) made available to the applicant in support of, or related to, any research endeavor, including a title, research grant, cooperative agreement, contract, institutional award, access to a laboratory, or other resource, including materials, travel compensation, or work incentives.

''(b) PROHIBITION.—It shall be unlawful for any individual to knowingly—

''(1) prepare or submit a Federal grant application that fails to disclose the receipt of any outside compensation, including foreign compensation, by the individual, the value of which is not less than $1,000;

''(2) forge, counterfeit, or otherwise falsify a document for the purpose of obtaining a Federal grant; or

''(3) prepare, submit, or assist in the preparation or submission of a Federal grant application or document in connection with a Federal grant application that—

''(A) contains a material false statement;

''(B) contains a material misrepresentation; or

''(C) fails to disclose a material fact.

''(c) EXCEPTION.—Subsection (b) does not apply to an activity—

''(1) carried out in connection with a lawfully authorized investigative, protective, or intelligence activity of—

''(A) a law enforcement agency; or

''(B) a Federal intelligence agency; or

''(2) authorized under chapter 224.

''(d) PENALTY.—Any individual who violates subsection (b)—

''(1) shall be fined in accordance with this title, imprisoned for not more than 5 years, or both, in accordance with the level of severity of that individual's violation of subsection (b); and

''(2) shall be prohibited from receiving a Federal grant during the 5-year period beginning on the date on which a sentence is imposed on the individual under paragraph (1).''.

(b) CLERICAL AMENDMENT.—The analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

''1041. Federal grant application fraud.''.

SEC. ___04. RESTRICTING THE ACQUISITION OF EMERGING TECHNOLOGIES BY CERTAIN ALIENS.

(a) IN GENERAL.—The Secretary of State may impose the sanctions described in subsection (c) if the Secretary determines an alien is seeking to enter the United States to knowingly acquire sensitive or emerging technologies to undermine national security interests of the United States by benefitting an adversarial foreign government's security or strategic capabilities.

(b) RELEVANT FACTORS.—To determine whether to impose sanctions under subsection (a), the Secretary of State shall—

(1) take account of information and analyses relevant to implementing subsection (a) from the Office of the Director of National Intelligence, the Department of Health and Human Services, the Department of Defense, the Department of Homeland Security, the Department of Energy, the Department of Commerce, and other appropriate Federal agencies;

(2) take account of the continual expert assessments of evolving sensitive or emerging technologies that foreign adversaries are targeting;

(3) take account of relevant information concerning the foreign person's employment or collaboration, to the extent known, with—

(A) foreign military and security related organizations that are adversarial to the United States;

(B) foreign institutions involved in the theft of United States research;

(C) entities involved in export control violations or the theft of intellectual property;

(D) a government that seeks to undermine the integrity and security of the United States research community; or

(E) other associations or collaborations that pose a national security threat based on intelligence assessments; and

(4) weigh the proportionality of risks and the factors listed in paragraphs (1) through (3).

(c) SANCTIONS DESCRIBED.—The sanctions described in this subsection are the following:

(1) INELIGIBILITY FOR VISAS AND ADMISSION TO THE UNITED STATES.—An alien described in subsection (a) may be—

(A) inadmissible to the United States;

(B) ineligible to receive a visa or other documentation to enter the United States; and

(C) otherwise ineligible to be admitted or paroled into the United States or to receive any other benefit under the Immigration and Nationality Act (8 U.S.C. 1101 et seq.).

(2) CURRENT VISAS REVOKED.—

(A) IN GENERAL.—An alien described in subsection (a) is subject to revocation of any visa or other entry documentation regardless of when the visa or other entry documentation is or was issued.

(B) IMMEDIATE EFFECT.—A revocation under clause (A) shall take effect immediately, and automatically cancel any other valid visa or entry documentation that is in the alien's possession, in accordance with section 221(i) of the Immigration and Nationality Act.

(3) EXCEPTION TO COMPLY WITH INTERNATIONAL OBLIGATIONS.—The sanctions described in this subsection shall not apply with respect to an alien if admitting or paroling the alien into the United States is necessary to permit the United States to comply with the Agreement regarding the Headquarters of the United Nations, signed at Lake Success June 26, 1947, and entered into force November 21, 1947, between the United Nations and the United States, or other applicable international obligations.

(d) REPORTING REQUIREMENT.—Not later than 180 days after the date of the enactment of this Act, and semi-annually thereafter until the sunset date set forth in subsection (f), the Secretary of State, in coordination with the Director of National Intelligence, the Director of the Office of Science and Technology Policy, the Secretary of Homeland Security, the Secretary of Defense, the Secretary of Energy, the Secretary of Commerce, and the heads of other appropriate Federal agencies, shall submit a report to the Committee on the Judiciary of the Senate, the Committee on Foreign Relations of the Senate, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Foreign Affairs of the House of Representatives, and the Committee on Oversight and Reform of the House of Representatives that identifies—

(1) any criteria, if relevant used to describe the alien in subsection (a);

(2) the number of individuals determined to be subject to sanctions under subsection (a), including the nationality of each such individual and the reasons for each sanctions determination; and

(3) the number of days from the date of the consular interview until a final decision is issued for each application for a visa considered under this section, listed by applicants' country of citizenship and relevant consulate.

(e) CLASSIFICATION OF REPORT.—Each report required under subsection (d) shall be submitted, to the extent practicable, in an unclassified form, but may be accompanied by a classified annex.

(f) SUNSET.—This section shall cease to be effective on the date that is 2 years after the date of the enactment of this Act.

SA 5811. Mr. PORTMAN (for himself and Mr. PETERS) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. CISA TECHNICAL CORRECTIONS AND IMPROVEMENTS.

(a) TECHNICAL AMENDMENT RELATING TO DOTGOV ACT OF 2020.—

(1) AMENDMENT.—Section 904(b)(1) of the DOTGOV Act of 2020 (title IX of division U of Public Law 116–260) is amended, in the matter preceding subparagraph (A), by striking ''Homeland Security Act'' and inserting ''Homeland Security Act of 2002''.

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

(b) CONSOLIDATION OF DEFINITIONS.—

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

''SEC. 2200. DEFINITIONS.

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

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

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

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

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

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

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

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

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

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

critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

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

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

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

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

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

''(D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

''(E) malicious cyber command and control;

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

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

''(H) any combination thereof.

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

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

''(A) means threats to and vulnerabilities of information or information systems and any related consequences caused by or resulting from unauthorized access, use, disclosure, degradation, disruption, modification, or destruction of such information or information systems, including such related consequences caused by an act of terrorism; and

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

''(9) CYBERSECURITY THREAT.—

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

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

''(10) DEFENSIVE MEASURE.—

''(A) IN GENERAL.—Except as provided in subparagraph (B), the term 'defensive measure' means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

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

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

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

''(11) DIRECTOR.—The term 'Director' means the Director Cybersecurity and Infrastructure Security Agency

''(12) HOMELAND SECURITY ENTERPRISE.—The term 'Homeland Security Enterprise' means relevant governmental and nongovernmental entities involved in homeland security, including Federal, State, local, and Tribal government officials, private sector representatives, academics, and other policy experts.

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

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

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

''(B) communicating or disclosing critical infrastructure information, including cybersecurity risks and incidents, to help prevent, detect, mitigate, or recover from the effects of an interference, a compromise, or an incapacitation problem related to critical infrastructure, including cybersecurity risks and incidents, or protected systems; and

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

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

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

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

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

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

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

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

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

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

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

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

''(21) SECURITY CONTROL.—The term 'security control' means the management, operational, and technical controls used to protect against an unauthorized effort to adversely affect the confidentiality, integrity, and availability of an information system or its information.

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

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

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

(A) by amending section 2201 (6 U.S.C. 651) to read as follows:

''SEC. 2201. DEFINITION.

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

(B) in section 2202 (6 U.S.C. 652)—

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

(ii) in subsection (b)(1), by striking ''in this subtitle referred to as the 'Director')''; and

(iii) in subsection (f)—

(I) in paragraph (1), by inserting ''Executive'' before ''Assistant Director''; and

(II) in paragraph (2), by inserting ''Executive'' before ''Assistant Director'';

(C) in section 2209 (6 U.S.C. 659)—

(i) by striking subsection (a);

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

(iii) in subsection (c)(1), as so redesignated—

(I) in subparagraph (A)(iii), as so redesignated, by striking '', as that term is defined under section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4))''; and

(II) in subparagraph (B)(ii), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

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

(I) in the matter preceding paragraph (1), by striking ''subsection (c)'' and inserting ''subsection (b)''; and

(II) in paragraph (1)(E)(ii)(II), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

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

(vi) by redesignating the first subsections (p) and (q) and second subsections (p) and (q) as subsections (o) and (p) and subsections (q) and (r), respectively; and

(vii) in subsection (o), as so redesignated—

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

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

(D) in section 2210 (6 U.S.C. 660)—

(i) by striking subsection (a);

(ii) by redesignating subsections (b) through (e) as subsections (a) through (d), respectively;

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

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

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

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

(E) in section 2211 (6 U.S.C. 661), by striking subsection (h);

(F) in section 2212 (6 U.S.C. 662), by striking ''information sharing and analysis organizations (as defined in section 2222(5))'' and inserting ''Information Sharing and Analysis Organizations'';

(G) in section 2213 (6 U.S.C. 663)—

(i) by striking subsection (a);

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

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

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

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

(I) in paragraph (1)—

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

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

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

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

(H) in section 2216 (6 U.S.C. 665b)—

(i) in subsection (d)(2), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations''; and

(ii) by striking subsection (f) and inserting the following:

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

(I) in section 2218(c)(4)(A) (6 U.S.C. 665d(4)(A)), by striking ''information sharing and analysis organizations'' and inserting ''Information Sharing and Analysis Organizations'';

(J) in section 2220A (6 U.S.C. 665g)—

(i) in subsection (a)—

(I) by striking paragraphs (1), (2), (5), and (6); and

(II) by redesignating paragraphs (3), (4), (7), (8), (9), (10), (11), and (12) as paragraphs (1) through (8), respectively;

(ii) in subsection (e)(2)(B)(xiv)(II)(aa), by striking ''information sharing and analysis organization'' and inserting ''Information Sharing and Analysis Organization'';

(iii) in subsection (p), by striking ''appropriate committees of Congress'' and inserting ''appropriate congressional committees''; and

(iv) in subsection (q)(4), in the matter preceding clause (i), by striking ''appropriate committees of Congress'' and inserting ''appropriate congressional committees''

(K) in section 2220C(f) (6 U.S.C. 665i(f))—

(i) by striking paragraph (1);

(ii) by redesignating paragraphs (2) and (3) as paragraphs (1) and (2), respectively; and

(iii) in paragraph (2), as so redesignated, by striking ''(enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9))'' and inserting ''(6 U.S.C. 1501)''; and

(L) in section 2222 (6 U.S.C. 671)—

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

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

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

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

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

''Sec. 2200. Definitions.'';

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

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

(C) by moving the item relating to section 2220D to appear after the item relating to section 2220C.

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

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

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

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

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

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

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

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

(C) by striking paragraphs (16) and (17) and inserting the following:

''(16) SECURITY CONTROL.—The term 'security control' has the meaning given the term in section 2200 of the Homeland Security Act of 2002.

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

(c) ADDITIONAL TECHNICAL AND CONFORMING AMENDMENTS.—

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

(A) in section 222 (6 U.S.C. 1521)—

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

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

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

(C) in section 226 (6 U.S.C. 1524)—

(i) in subsection (a)—

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

(II) in paragraph (2), by striking ''section 102'' and inserting ''section 2200 of the Homeland Security Act of 2002'';

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

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

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

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

(2) PUBLIC HEALTH SERVICE ACT.—Section 2811(b)(4)(D) of the Public Health Service Act (42 U.S.C. 300hh–10(b)(4)(D)) is amended by striking ''section 228(c) of the Homeland Security Act of 2002 (6 U.S.C. 149(c))'' and inserting ''section 2210(b) of the Homeland Security Act of 2002 (6 U.S.C. 660(b))''.

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

(A) in subsection (a)—

(i) by striking paragraph (5);

(ii) by redesignating paragraphs (6) and (7) as paragraphs (5) and (6), respectively;

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

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

(B) in subsection (c)(3)(B), by striking ''section 2201(5)'' and inserting ''section 2200''; and

(C) in subsection (d), by striking ''section 2215 of the Homeland Security Act of 2002, as added by this section'' and inserting ''section 2218 of the Homeland Security Act of 2002 (6 U.S.C. 665d)''.

(4) NATIONAL SECURITY ACT OF 1947.—Section 113B(b)(4) of the National Security Act of 1947 (50 U.S.C. 3049a(b)(4)) is amended by striking section ''226 of the Homeland Security Act of 2002 (6 U.S.C. 147)'' and inserting ''section 2208 of the Homeland Security Act of 2002 (6 U.S.C. 658)''.

(5) IOT CYBERSECURITY IMPROVEMENT ACT OF 2020.—Section 5(b)(3) of the IoT Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g–3c(b)(3)) is amended by striking ''section 2209(m) of the Homeland Security Act of 2002 (6 U.S.C. 659(m))'' and inserting ''section 2209(l) of the Homeland Security Act of 2002 (6 U.S.C. 659(l))''.

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

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

SA 5812. Ms. KLOBUCHAR (for herself and Mr. TILLIS) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following: