and I believe Senator REED and I are moving forward with some amendments we can have debated and also voted on today.

CONCLUSION OF MORNING BUSINESS

The PRESIDING OFFICER. Morning business is closed.

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2016

The PRESIDING OFFICER. Under the previous order, the Senate will resume consideration of H.R. 1735, which the clerk will report.

The legislative clerk read as follows:

A bill (H.R. 1735) to authorize appropriations for fiscal year 2016 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.

Pending:

McCain amendment No. 1463, in the nature of a substitute.

McCain amendment No. 1456 (to amendment No. 1463), to require additional information supporting long-range plans for construction of naval vessels.

Cornyn amendment No. 1486 (to amendment No. 1463), to require reporting on energy security issues involving Europe and the Russian Federation, and to express the sense of Congress regarding ways the United States could help vulnerable allies and partners with energy security.

Vitter amendment No. 1473 (to amendment No. 1463), to limit the retirement of Army combat units.

Markey amendment No. 1645 (to amendment No. 1463), to express the sense of Congress that exports of crude oil to United States allies and partners should not be determined to be consistent with the national interest if those exports would increase energy prices in the United States for American consumers or businesses or increase the reliance of the United States on imported oil.

Reed (for Blumenthal) amendment No. 1564 (to amendment No. 1463), to increase civil penalties for violations of the Servicemembers Civil Relief Act.

McCain (for Paul) modified amendment No. 1543 (to amendment No. 1463), to strengthen employee cost savings suggestions programs within the Federal Government.

Reed (for Durbin) modified amendment No. 1559 (to amendment No. 1463), to prohibit the award of Department of Defense contracts to inverted domestic corporations.

McCain (for Burr) amendment No. 1569 (to amendment No. 1463), to ensure criminal background checks of employees of the military child care system and providers of child care services and youth program services for military dependents.

Feinstein (for McCain) amendment No. 1889 (to amendment No. 1463), to reaffirm the prohibition on torture.

Fischer/Booker amendment No. 1825 (to amendment No. 1463), to authorize appropriations for national security aspects of the Merchant Marine for fiscal years 2016 and 2017.

Burr/McCain amendment No. 1921 (to amendment No. 1569), to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats.

Mr. MCCAIN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Ms. MIKULSKI. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Ms. MIKULSKI. Mr. President, I was first going to offer an amendment, but both the chairman and ranking member of the committee suggested that I wait until after they have had a chance to review some of the technical details. So I will speak on an amendment that I will in all probability offer at a later time.

My amendment really goes to how we make sure we help our troops with the many stresses that are in their lives. My goal is to add money to funding our commissaries. This amendment, which I will offer at a later time, restores $322 million in cuts to commissaries proposed by the Department of Defense. It would authorize $1.4 billion in funding—the same level that is in the House National Defense Authorization Act and in the House Defense appropriations bill. It offsets the $322 million for commissaries by reducing the Pentagon's budget in failed policies to buy spare parts. They have a lot of waste there, and we think we can find the $322 million we need there, and that is the technical issue we need to work, also known as the offset. But what is not technical is the fact that we have to make sure our commissaries function at their current level.

Commissaries represent one of the most significant and lasting benefits for military members and their families. Commissaries have been around since 1826, giving military families the ability to shop at a network of stores. The commissary system is simple. If you are Active Duty, Reserve, National Guard, or a retired member of the family, you have access to 246 commissaries worldwide. They are particularly important to many of our troops overseas, and they give military families affordable access to healthy foods.

The benefits of commissaries are significant. They feed those people who are actually members of our military. They help military families stretch their budgets, and they also help provide jobs to family members in the military who work in those commissaries.

Our distinguished colleagues on the authorizing committee, Senator MCCAIN and Senator JACK REED, are themselves military men. Senator MCCAIN is a graduate of the Naval Academy and Senator JACK REED graduated from West Point. They know that one of the big expenditures right now for our military is rising health costs. The military itself is looking at how to make sure they keep our troops healthy not only while they are doing their job but also how to keep them healthy so that when they move on, they will be in excellent shape. The commissaries do those kinds of things. They provide what grocery stores provide—fresh fruits and vegetables. They provide healthy foods.

Also, for example, my own commissary at Fort Meade, which is part of the Healthy Base Initiative, has shown people how to stretch their dollar more so they can get more for their family budget and also has actual recommendations on how to add nutrition—save money and add nutrition. If we want to bend the health care cost curve, while we are looking at important medical research, research shows that good food leads to good health.

The other thing is this: Military members get a significant savings from commissaries. The average savings is about 30 percent on a grocery bill. For a family of four, that comes to over $4,000 a year. Everyone knows how much military families are stretched, and for our men and women who are enlisted, this is a really big deal. We need to make this available for them.

What many people don't realize is that the commissaries not only create jobs, but 60 percent of commissary workers are spouses of men who serve in the military. About 100,000 jobs are supported through commissaries. The other thing the DOD wants to do is cut their hours. Well, if they cut their hours, that does cut jobs, but it also cuts opportunity.

When you are in the military, you work around the clock. You are not on the clock; you work around the clock. So if you are a military police officer, you could be getting off of duty late at night. If you are someone who repairs our helicopters or airplanes, you could be getting off at night.

The commissary at Fort Meade serves agencies such as the National Security Agency. They essentially work a 36-hour day. They work around the clock, 24 hours a day. Our commissary isn't open 24 hours a day, but I can tell you it can't be open from 10 a.m. to 4 p.m. and still meet the needs of our military workforce.

The Department of Defense wants to make the commissaries more self-sustaining, and we don't argue with that. We can always find efficiencies and look at new ways to do things. But don't cut $322 million and further cut it close to $1 billion over the next 4 years.

What we want to do is make sure our military families have what they need. First of all, we want them to have good food. We want them to be able to go to these commissaries at hours that work for military families. We also want to look at the long-range effects of bending the health care curve.

I am going to come back to the commissary at Fort Meade. I am very proud of the fact that Fort Meade is what we call a compassionate post. That means if you are in the U.S. Army and you have a special needs child, one of the highly desirable places to be based is at Fort Meade. Why? Because Anne Arundel County has one of

the best programs for special education in the State and in the country. You also have access to Kennedy Krieger, which is one of the internationally iconic agencies that address the needs of children with not only special needs but multiple special needs.

We are very happy that Fort Meade is in Maryland and that it is known as a compassionate post. But think of those families who have a child with cerebral palsy or multiple complications that might even require the child to constantly need a respirator. All of these things go on along with the stress of being a military family. We can certainly keep the commissaries open so that they can get the food they need for their families and have the commissaries open during the hours that work for them. This is what real life in the military is.

After Desert Storm, I remember when the Appropriations Committee met under the leadership of Senator Byrd and Senator Ted Steven. They asked General Schwarzkopf what he needed in an after-action report. He said: We need better intelligence. And we worked really hard to upgrade to where we are. He also said: We need better food. We need better food for our troops, and people need to believe their families are being taken care of while they are in harm's way.

We ask a lot from our military, and our military families are now asking us: Don't cut the commissaries. Keep them open. Keep them affordable. Keep them available. Once we clarify the technicalities of the offset, which is required, I will come back and offer my amendment, which I hope will pass the Senate with a 100-to-0 vote.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. CORNYN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

AMENDMENT NO. 1569, AS MODIFIED

Mr. MCCAIN. Mr. President, I modify my amendment No. 1569 by accepting the second-degree amendment No. 1921, offered by the Senator from North Carolina.

The PRESIDING OFFICER. The Senator has that right. The amendment is so modified.

The amendment, as modified, is as follows:

At the end of subtitle F of title V, add the following:

TITLE XVII—CYBERSECURITY INFORMATION SHARING

SECTION 1701. SHORT TITLE.

This title may be cited as the ''Cybersecurity Information Sharing Act of 2015''.

SEC. 1702. DEFINITIONS.

In this title:

(1) AGENCY.—The term ''agency'' has the meaning given the term in section 3502 of title 44, United States Code.

(2) ANTITRUST LAWS.—The term ''antitrust laws''—

(A) has the meaning given the term in section 1 of the Clayton Act (15 U.S.C. 12);

(B) includes section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section 5 of that Act applies to unfair methods of competition; and

(C) includes any State law that has the same intent and effect as the laws under subparagraphs (A) and (B).

(3) APPROPRIATE FEDERAL ENTITIES.—The term ''appropriate Federal entities'' means the following:

(A) The Department of Commerce.

(B) The Department of Defense.

(C) The Department of Energy.

(D) The Department of Homeland Security.

(E) The Department of Justice.

(F) The Department of the Treasury.

(G) The Office of the Director of National Intelligence.

(4) 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.

(5) 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.

(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) 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, or substantially harms an information system or data on an information system not belonging to—

(i) the private 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.

(8) ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''entity'' means any private entity, non-Federal government agency or department, or State, tribal, or local government (including a political subdivision, department, or component thereof).

(B) INCLUSIONS.—The term ''entity'' includes a government agency or department of the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

(C) EXCLUSION.—The term ''entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(9) FEDERAL ENTITY.—The term ''Federal entity'' means a department or agency of the United States or any component of such department or agency.

(10) INFORMATION SYSTEM.—The term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

(11) LOCAL GOVERNMENT.—The term ''local government'' means any borough, city, county, parish, town, township, village, or other political subdivision of a State.

(12) MALICIOUS CYBER COMMAND AND CONTROL.—The term ''malicious cyber command and control'' means a method for unauthorized remote identification of, access to, or use of, an information system or information that is stored on, processed by, or transiting an information system.

(13) MALICIOUS RECONNAISSANCE.—The term ''malicious reconnaissance'' means a method for actively probing or passively monitoring an information system for the purpose of discerning security vulnerabilities of the information system, if such method is associated with a known or suspected cybersecurity threat.

(14) 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.

(15) PRIVATE ENTITY.—

(A) IN GENERAL.—Except as otherwise provided in this paragraph, the term ''private entity'' means any person or private group, organization, proprietorship, partnership, trust, cooperative, corporation, or other commercial or nonprofit entity, including an officer, employee, or agent thereof.

(B) INCLUSION.—The term ''private entity'' includes a State, tribal, or local government performing electric utility services.

(C) EXCLUSION.—The term ''private entity'' does not include a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(16) 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.

(17) 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.

(18) TRIBAL.—The term ''tribal'' has the meaning given the term ''Indian tribe'' in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 450b).

SEC. 1703. SHARING OF INFORMATION BY THE FEDERAL GOVERNMENT.

(a) IN GENERAL.—Consistent with the protection of classified information, intelligence sources and methods, and privacy and civil liberties, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall develop and promulgate procedures to facilitate and promote—

(1) the timely sharing of classified cyber threat indicators in the possession of the Federal Government with cleared representatives of relevant entities;

(2) the timely sharing with relevant entities of cyber threat indicators or information in the possession of the Federal Government that may be declassified and shared at an unclassified level;

(3) the sharing with relevant entities, or the public if appropriate, of unclassified, including controlled unclassified, cyber threat indicators in the possession of the Federal Government; and

(4) the sharing with entities, if appropriate, of information in the possession of the Federal Government about cybersecurity threats to such entities to prevent or mitigate adverse effects from such cybersecurity threats.

(b) DEVELOPMENT OF PROCEDURES.—

(1) IN GENERAL.—The procedures developed and promulgated under subsection (a) shall—

(A) ensure the Federal Government has and maintains the capability to share cyber threat indicators in real time consistent with the protection of classified information;

(B) incorporate, to the greatest extent practicable, existing processes and existing roles and responsibilities of Federal and non-Federal entities for information sharing by the Federal Government, including sector specific information sharing and analysis centers;

(C) include procedures for notifying entities that have received a cyber threat indicator from a Federal entity under this title that is known or determined to be in error or in contravention of the requirements of this title or another provision of Federal law or policy of such error or contravention;

(D) include requirements for Federal entities receiving cyber threat indicators or defensive measures to implement and utilize security controls to protect against unauthorized access to or acquisition of such cyber threat indicators or defensive measures; and

(E) include procedures that require a Federal entity, prior to the sharing of a cyber threat indicator—

(i) to review such cyber threat indicator to assess whether such cyber threat indicator contains any information that such Federal entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(ii) to implement and utilize a technical capability configured to remove any personal information of or identifying a specific person not directly related to a cybersecurity threat.

(2) COORDINATION.—In developing the procedures required under this section, the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General shall coordinate with appropriate Federal entities, including the National Laboratories (as defined in section 1702 of the Energy Policy Act of 2005 (42 U.S.C. 15801)), to ensure that effective protocols are implemented that will facilitate and promote the sharing of cyber threat indicators by the Federal Government in a timely manner.

(c) SUBMITTAL TO CONGRESS.—Not later than 60 days after the date of the enactment of this title, the Director of National Intelligence, in consultation with the heads of the appropriate Federal entities, shall submit to Congress the procedures required by subsection (a).

SEC. 1704. AUTHORIZATIONS FOR PREVENTING, DETECTING, ANALYZING, AND MITIGATING CYBERSECURITY THREATS.

(a) AUTHORIZATION FOR MONITORING.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

(A) an information system of such private entity;

(B) an information system of another entity, upon the authorization and written consent of such other entity;

(C) an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and

(D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or

(B) to limit otherwise lawful activity.

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

(1) IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

(A) an information system of such private entity in order to protect the rights or property of the private entity;

(B) an information system of another entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

(C) an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

(2) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the use of a defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(c) AUTHORIZATION FOR SHARING OR RECEIVING CYBER THREAT INDICATORS OR DEFENSIVE MEASURES.—

(1) IN GENERAL.—Except as provided in paragraph (2) and notwithstanding any other provision of law, an entity may, for the purposes permitted under this title and consistent with the protection of classified information, share with, or receive from, any other entity or the Federal Government a cyber threat indicator or defensive measure.

(2) LAWFUL RESTRICTION.—An entity receiving a cyber threat indicator or defensive measure from another entity or Federal entity shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity or Federal entity.

(3) CONSTRUCTION.—Nothing in this subsection shall be construed—

(A) to authorize the sharing or receiving of a cyber threat indicator or defensive measure other than as provided in this subsection; or

(B) to limit otherwise lawful activity.

(d) PROTECTION AND USE OF INFORMATION.—

(1) SECURITY OF INFORMATION.—An entity monitoring an information system, operating a defensive measure, or providing or receiving a cyber threat indicator or defensive measure under this section shall implement and utilize a security control to protect against unauthorized access to or acquisition of such cyber threat indicator or defensive measure.

(2) REMOVAL OF CERTAIN PERSONAL INFORMATION.—An entity sharing a cyber threat indicator pursuant to this title shall, prior to such sharing—

(A) review such cyber threat indicator to assess whether such cyber threat indicator contains any information that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat and remove such information; or

(B) implement and utilize a technical capability configured to remove any information contained within such indicator that the entity knows at the time of sharing to be personal information of or identifying a specific person not directly related to a cybersecurity threat.

(3) USE OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES BY ENTITIES.—

(A) IN GENERAL.—Consistent with this title, a cyber threat indicator or defensive measure shared or received under this section may, for cybersecurity purposes—

(i) be used by an entity to monitor or operate a defensive measure on—

(I) an information system of the entity; or

(II) an information system of another entity or a Federal entity upon the written consent of that other entity or that Federal entity; and

(ii) be otherwise used, retained, and further shared by an entity subject to—

(I) an otherwise lawful restriction placed by the sharing entity or Federal entity on such cyber threat indicator or defensive measure; or

(II) an otherwise applicable provision of law.

(B) CONSTRUCTION.—Nothing in this paragraph shall be construed to authorize the use of a cyber threat indicator or defensive measure other than as provided in this section.

(4) USE OF CYBER THREAT INDICATORS BY STATE, TRIBAL, OR LOCAL GOVERNMENT.—

(A) LAW ENFORCEMENT USE.—

(i) PRIOR WRITTEN CONSENT.—Except as provided in clause (ii), a cyber threat indicator shared with a State, tribal, or local government under this section may, with the prior written consent of the entity sharing such indicator, be used by a State, tribal, or local government for the purpose of preventing, investigating, or prosecuting any of the offenses described in section 1705(d)(5)(A)(vi).

(ii) ORAL CONSENT.—If exigent circumstances prevent obtaining written consent under clause (i), such consent may be provided orally with subsequent documentation of the consent.

(B) EXEMPTION FROM DISCLOSURE.—A cyber threat indicator shared with a State, tribal, or local government under this section shall be—

(i) deemed voluntarily shared information; and

(ii) exempt from disclosure under any State, tribal, or local law requiring disclosure of information or records.

(C) STATE, TRIBAL, AND LOCAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), a cyber threat indicator or defensive measure shared with a State, tribal, or local government under this title shall not be directly used by any State, tribal, or local government to regulate, including an enforcement action, the lawful activity of any entity, including an activity relating to monitoring, operating a defensive measure, or sharing of a cyber threat indicator.

(ii) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—A cyber threat indicator or defensive measures shared as described in clause (i) may, consistent with a State, tribal, or local government regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of a regulation relating to such information systems.

(e) ANTITRUST EXEMPTION.—

(1) IN GENERAL.—Except as provided in section 1708(e), it shall not be considered a violation of any provision of antitrust laws for 2 or more private entities to exchange or provide a cyber threat indicator, or assistance relating to the prevention, investigation, or mitigation of a cybersecurity threat, for cybersecurity purposes under this title.

(2) APPLICABILITY.—Paragraph (1) shall apply only to information that is exchanged or assistance provided in order to assist with—

(A) facilitating the prevention, investigation, or mitigation of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system; or

(B) communicating or disclosing a cyber threat indicator to help prevent, investigate, or mitigate the effect of a cybersecurity threat to an information system or information that is stored on, processed by, or transiting an information system.

(f) NO RIGHT OR BENEFIT.—The sharing of a cyber threat indicator with an entity under this title shall not create a right or benefit to similar information by such entity or any other entity.

SEC. 1705. SHARING OF CYBER THREAT INDICATORS AND DEFENSIVE MEASURES WITH THE FEDERAL GOVERNMENT.

(a) REQUIREMENT FOR POLICIES AND PROCEDURES.—

(1) INTERIM POLICIES AND PROCEDURES.—Not later than 60 days after the date of the enactment of this title, the Attorney General, in coordination with the heads of the appropriate Federal entities, shall develop and submit to Congress interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(2) FINAL POLICIES AND PROCEDURES.—Not later than 180 days after the date of the enactment of this title, the Attorney General shall, in coordination with the heads of the appropriate Federal entities, promulgate final policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government.

(3) REQUIREMENTS CONCERNING POLICIES AND PROCEDURES.—Consistent with the guidelines required by subsection (b), the policies and procedures developed and promulgated under this subsection shall—

(A) ensure that cyber threat indicators are shared with the Federal Government by any entity pursuant to section 1704(c) through the real-time process described in subsection (c) of this section—

(i) are shared in an automated manner with all of the appropriate Federal entities;

(ii) are not subject to any delay, modification, or any other action that could impede real-time receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(B) ensure that cyber threat indicators shared with the Federal Government by any entity pursuant to section 1704 in a manner other than the real-time process described in subsection (c) of this section—

(i) are shared as quickly as operationally practicable with all of the appropriate Federal entities;

(ii) are not subject to any unnecessary delay, interference, or any other action that could impede receipt by all of the appropriate Federal entities; and

(iii) may be provided to other Federal entities;

(C) consistent with this title, any other applicable provisions of law, and the fair information practice principles set forth in appendix A of the document entitled ''National Strategy for Trusted Identities in Cyberspace'' and published by the President in April 2011, govern the retention, use, and dissemination by the Federal Government of cyber threat indicators shared with the Federal Government under this title, including the extent, if any, to which such cyber threat indicators may be used by the Federal Government; and

(D) ensure there is—

(i) an audit capability; and

(ii) appropriate sanctions in place for officers, employees, or agents of a Federal entity who knowingly and willfully conduct activities under this title in an unauthorized manner.

(4) GUIDELINES FOR ENTITIES SHARING CYBER THREAT INDICATORS WITH FEDERAL GOVERNMENT.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this title, the Attorney General shall develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities under this title.

(B) CONTENTS.—The guidelines developed and made publicly available under subparagraph (A) shall include guidance on the following:

(i) Identification of types of information that would qualify as a cyber threat indicator under this title that would be unlikely to include personal information of or identifying a specific person not directly related to a cyber security threat.

(ii) Identification of types of information protected under otherwise applicable privacy laws that are unlikely to be directly related to a cybersecurity threat.

(iii) Such other matters as the Attorney General considers appropriate for entities sharing cyber threat indicators with Federal entities under this title.

(b) PRIVACY AND CIVIL LIBERTIES.—

(1) GUIDELINES OF ATTORNEY GENERAL.—Not later than 60 days after the date of the enactment of this title, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1), develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(2) FINAL GUIDELINES.—

(A) IN GENERAL.—Not later than 180 days after the date of the enactment of this title, the Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers designated under section 1062 of the National Security Intelligence Reform Act of 2004 (42 U.S.C. 2000ee–1) and such private entities with industry expertise as the Attorney General considers relevant, promulgate final guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity obtained in connection with activities authorized in this title.

(B) PERIODIC REVIEW.—The Attorney General shall, in coordination with heads of the appropriate Federal entities and in consultation with officers and private entities described in subparagraph (A), periodically review the guidelines promulgated under subparagraph (A).

(3) CONTENT.—The guidelines required by paragraphs (1) and (2) shall, consistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—

(A) limit the impact on privacy and civil liberties of activities by the Federal Government under this title;

(B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of or identifying specific persons, including by establishing—

(i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this title; and

(ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;

(C) include requirements to safeguard cyber threat indicators containing personal information of or identifying specific persons from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines;

(D) include procedures for notifying entities and Federal entities if information received pursuant to this section is known or determined by a Federal entity receiving such information not to constitute a cyber threat indicator;

(E) protect the confidentiality of cyber threat indicators containing personal information of or identifying specific persons to the greatest extent practicable and require recipients to be informed that such indicators may only be used for purposes authorized under this title; and

(F) include steps that may be needed so that dissemination of cyber threat indicators is consistent with the protection of classified and other sensitive national security information.

(c) CAPABILITY AND PROCESS WITHIN THE DEPARTMENT OF HOMELAND SECURITY.—

(1) IN GENERAL.—Not later than 90 days after the date of the enactment of this title, the Secretary of Homeland Security, in coordination with the heads of the appropriate Federal entities, shall develop and implement a capability and process within the Department of Homeland Security that—

(A) shall accept from any entity in real time cyber threat indicators and defensive measures, pursuant to this section;

(B) shall, upon submittal of the certification under paragraph (2) that such capability and process fully and effectively operates as described in such paragraph, be the process by which the Federal Government receives cyber threat indicators and defensive measures under this title that are shared by a private entity with the Federal Government through electronic mail or media, an interactive form on an Internet website, or a real time, automated process between information systems except—

(i) communications between a Federal entity and a private entity regarding a previously shared cyber threat indicator; and

(ii) communications by a regulated entity with such entity's Federal regulatory authority regarding a cybersecurity threat;

(C) ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators shared through the real-time process within the Department of Homeland Security;

(D) is in compliance with the policies, procedures, and guidelines required by this section; and

(E) does not limit or prohibit otherwise lawful disclosures of communications, records, or other information, including—

(i) reporting of known or suspected criminal activity, by an entity to any other entity or a Federal entity;

(ii) voluntary or legally compelled participation in a Federal investigation; and

(iii) providing cyber threat indicators or defensive measures as part of a statutory or authorized contractual requirement.

(2) CERTIFICATION.—Not later than 10 days prior to the implementation of the capability and process required by paragraph (1), the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, certify to Congress whether such capability and process fully and effectively operates—

(A) as the process by which the Federal Government receives from any entity a cyber threat indicator or defensive measure under this title; and

(B) in accordance with the policies, procedures, and guidelines developed under this section.

(3) PUBLIC NOTICE AND ACCESS.—The Secretary of Homeland Security shall ensure there is public notice of, and access to, the capability and process developed and implemented under paragraph (1) so that—

(A) any entity may share cyber threat indicators and defensive measures through such process with the Federal Government; and

(B) all of the appropriate Federal entities receive such cyber threat indicators and defensive measures in real time with receipt through the process within the Department of Homeland Security.

(4) OTHER FEDERAL ENTITIES.—The process developed and implemented under paragraph (1) shall ensure that other Federal entities receive in a timely manner any cyber threat indicators and defensive measures shared with the Federal Government through such process.

(5) REPORT ON DEVELOPMENT AND IMPLEMENTATION.—

(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this title, the Secretary of Homeland Security shall submit to Congress a report on the development and implementation of the capability and process required by paragraph (1), including a description of such capability and process and the public notice of, and access to, such process.

(B) CLASSIFIED ANNEX.—The report required by subparagraph (A) shall be submitted in unclassified form, but may include a classified annex.

(d) INFORMATION SHARED WITH OR PROVIDED TO THE FEDERAL GOVERNMENT.—

(1) NO WAIVER OF PRIVILEGE OR PROTECTION.—The provision of cyber threat indicators and defensive measures to the Federal Government under this title shall not constitute a waiver of any applicable privilege or protection provided by law, including trade secret protection.

(2) PROPRIETARY INFORMATION.—Consistent with section 1704(c)(2), a cyber threat indicator or defensive measure provided by an entity to the Federal Government under this title shall be considered the commercial, financial, and proprietary information of such entity when so designated by the originating entity or a third party acting in accordance with the written authorization of the originating entity.

(3) EXEMPTION FROM DISCLOSURE.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(4) EX PARTE COMMUNICATIONS.—The provision of a cyber threat indicator or defensive measure to the Federal Government under this title shall not be subject to a rule of any Federal agency or department or any judicial doctrine regarding ex parte communications with a decisionmaking official.

(5) DISCLOSURE, RETENTION, AND USE.—

(A) AUTHORIZED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may be disclosed to, retained by, and used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, component, officer, employee, or agent of the Federal Government solely for—

(i) a cybersecurity purpose;

(ii) the purpose of identifying a cybersecurity threat, including the source of such cybersecurity threat, or a security vulnerability;

(iii) the purpose of identifying a cybersecurity threat involving the use of an information system by a foreign adversary or terrorist;

(iv) the purpose of responding to, or otherwise preventing or mitigating, an imminent threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(v) the purpose of responding to, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(vi) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in clause (iv) or any of the offenses listed in—

(I) section 3559(c)(2)(F) of title 18, United States Code (relating to serious violent felonies);

(II) sections 1028 through 1030 of such title (relating to fraud and identity theft);

(III) chapter 37 of such title (relating to espionage and censorship); and

(IV) chapter 90 of such title (relating to protection of trade secrets).

(B) PROHIBITED ACTIVITIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be disclosed to, retained by, or used by any Federal agency or department for any use not permitted under subparagraph (A).

(C) PRIVACY AND CIVIL LIBERTIES.—Cyber threat indicators and defensive measures provided to the Federal Government under this title shall be retained, used, and disseminated by the Federal Government—

(i) in accordance with the policies, procedures, and guidelines required by subsections (a) and (b);

(ii) in a manner that protects from unauthorized use or disclosure any cyber threat indicators that may contain personal information of or identifying specific persons; and

(iii) in a manner that protects the confidentiality of cyber threat indicators containing personal information of or identifying a specific person.

(D) FEDERAL REGULATORY AUTHORITY.—

(i) IN GENERAL.—Except as provided in clause (ii), cyber threat indicators and defensive measures provided to the Federal Government under this title shall not be directly used by any Federal, State, tribal, or local government to regulate, including an enforcement action, the lawful activities of any entity, including activities relating to monitoring, operating defensive measures, or sharing cyber threat indicators.

(ii) EXCEPTIONS.—

(I) REGULATORY AUTHORITY SPECIFICALLY RELATING TO PREVENTION OR MITIGATION OF CYBERSECURITY THREATS.—Cyber threat indicators and defensive measures provided to the Federal Government under this title may, consistent with Federal or State regulatory authority specifically relating to the prevention or mitigation of cybersecurity threats to information systems, inform the development or implementation of regulations relating to such information systems.

(II) PROCEDURES DEVELOPED AND IMPLEMENTED UNDER THIS TITLE.—Clause (i) shall not apply to procedures developed and implemented under this title.

SEC. 1706. PROTECTION FROM LIABILITY.

(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of information systems and information under section 1704(a) that is conducted in accordance with this title.

(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or defensive measures under section 1704(c) if—

(1) such sharing or receipt is conducted in accordance with this title; and

(2) in a case in which a cyber threat indicator or defensive measure is shared with the Federal Government, the cyber threat indicator or defensive measure is shared in a manner that is consistent with section 1705(c)(1)(B) and the sharing or receipt, as the case may be, occurs after the earlier of—

(A) the date on which the interim policies and procedures are submitted to Congress under section 1705(a)(1); or

(B) the date that is 60 days after the date of the enactment of this title.

(c) CONSTRUCTION.—Nothing in this section shall be construed—

(1) to require dismissal of a cause of action against an entity that has engaged in gross negligence or willful misconduct in the course of conducting activities authorized by this title; or

(2) to undermine or limit the availability of otherwise applicable common law or statutory defenses.

SEC. 1707. OVERSIGHT OF GOVERNMENT ACTIVITIES.

(a) BIENNIAL REPORT ON IMPLEMENTATION.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this title, and not less frequently than once every 2 years thereafter, the heads of the appropriate Federal entities shall jointly submit and the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy, in consultation with the Council of Inspectors General on Financial Oversight, shall jointly submit to Congress a

detailed report concerning the implementation of this title.

(2) CONTENTS.—Each report submitted under paragraph (1) shall include the following:

(A) An assessment of the sufficiency of the policies, procedures, and guidelines required by section 1705 in ensuring that cyber threat indicators are shared effectively and responsibly within the Federal Government.

(B) An evaluation of the effectiveness of real-time information sharing through the capability and process developed under section 1705(c), including any impediments to such real-time sharing.

(C) An assessment of the sufficiency of the procedures developed under section 1703 in ensuring that cyber threat indicators in the possession of the Federal Government are shared in a timely and adequate manner with appropriate entities, or, if appropriate, are made publicly available.

(D) An assessment of whether cyber threat indicators have been properly classified and an accounting of the number of security clearances authorized by the Federal Government for the purposes of this title.

(E) A review of the type of cyber threat indicators shared with the Federal Government under this title, including the following:

(i) The degree to which such information may impact the privacy and civil liberties of specific persons.

(ii) A quantitative and qualitative assessment of the impact of the sharing of such cyber threat indicators with the Federal Government on privacy and civil liberties of specific persons.

(iii) The adequacy of any steps taken by the Federal Government to reduce such impact.

(F) A review of actions taken by the Federal Government based on cyber threat indicators shared with the Federal Government under this title, including the appropriateness of any subsequent use or dissemination of such cyber threat indicators by a Federal entity under section 1705.

(G) A description of any significant violations of the requirements of this title by the Federal Government.

(H) A summary of the number and type of entities that received classified cyber threat indicators from the Federal Government under this title and an evaluation of the risks and benefits of sharing such cyber threat indicators.

(3) RECOMMENDATIONS.—Each report submitted under paragraph (1) may include recommendations for improvements or modifications to the authorities and processes under this title.

(4) FORM OF REPORT.—Each report required by paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(b) REPORTS ON PRIVACY AND CIVIL LIBERTIES.—

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Not later than 2 years after the date of the enactment of this title and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the effect on privacy and civil liberties by the type of activities carried out under this title; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 1705 in addressing concerns relating to privacy and civil liberties.

(2) BIENNIAL REPORT OF INSPECTORS GENERAL.—

(A) IN GENERAL.—Not later than 2 years after the date of the enactment of this title and not less frequently than once every 2 years thereafter, the Inspector General of the Department of Homeland Security, the Inspector General of the Intelligence Community, the Inspector General of the Department of Justice, the Inspector General of the Department of Defense, and the Inspector General of the Department of Energy shall, in consultation with the Council of Inspectors General on Financial Oversight, jointly submit to Congress a report on the receipt, use, and dissemination of cyber threat indicators and defensive measures that have been shared with Federal entities under this title.

(B) CONTENTS.—Each report submitted under subparagraph (A) shall include the following:

(i) A review of the types of cyber threat indicators shared with Federal entities.

(ii) A review of the actions taken by Federal entities as a result of the receipt of such cyber threat indicators.

(iii) A list of Federal entities receiving such cyber threat indicators.

(iv) A review of the sharing of such cyber threat indicators among Federal entities to identify inappropriate barriers to sharing information.

(3) RECOMMENDATIONS.—Each report submitted under this subsection may include such recommendations as the Privacy and Civil Liberties Oversight Board, with respect to a report submitted under paragraph (1), or the Inspectors General referred to in paragraph (2)(A), with respect to a report submitted under paragraph (2), may have for improvements or modifications to the authorities under this title.

(4) FORM.—Each report required under this subsection shall be submitted in unclassified form, but may include a classified annex.

SEC. 1708. CONSTRUCTION AND PREEMPTION.

(a) OTHERWISE LAWFUL DISCLOSURES.—Nothing in this title shall be construed—

(1) to limit or prohibit otherwise lawful disclosures of communications, records, or other information, including reporting of known or suspected criminal activity, by an entity to any other entity or the Federal Government under this title; or

(2) to limit or prohibit otherwise lawful use of such disclosures by any Federal entity, even when such otherwise lawful disclosures duplicate or replicate disclosures made under this title.

(b) WHISTLE BLOWER PROTECTIONS.—Nothing in this title shall be construed to prohibit or limit the disclosure of information protected under section 2302(b)(8) of title 5, United States Code (governing disclosures of illegality, waste, fraud, abuse, or public health or safety threats), section 7211 of title 5, United States Code (governing disclosures to Congress), section 1034 of title 10, United States Code (governing disclosure to Congress by members of the military), section 1104 of the National Security Act of 1947 (50 U.S.C. 3234) (governing disclosure by employees of elements of the intelligence community), or any similar provision of Federal or State law.

(c) PROTECTION OF SOURCES AND METHODS.—Nothing in this title shall be construed—

(1) as creating any immunity against, or otherwise affecting, any action brought by the Federal Government, or any agency or department thereof, to enforce any law, executive order, or procedure governing the appropriate handling, disclosure, or use of classified information;

(2) to affect the conduct of authorized law enforcement or intelligence activities; or

(3) to modify the authority of a department or agency of the Federal Government to protect classified information and sources and methods and the national security of the United States.

(d) RELATIONSHIP TO OTHER LAWS.—Nothing in this title shall be construed to affect any requirement under any other provision of law for an entity to provide information to the Federal Government.

(e) PROHIBITED CONDUCT.—Nothing in this title shall be construed to permit price-fixing, allocating a market between competitors, monopolizing or attempting to monopolize a market, boycotting, or exchanges of price or cost information, customer lists, or information regarding future competitive planning.

(f) INFORMATION SHARING RELATIONSHIPS.—Nothing in this title shall be construed—

(1) to limit or modify an existing information sharing relationship;

(2) to prohibit a new information sharing relationship;

(3) to require a new information sharing relationship between any entity and the Federal Government; or

(4) to require the use of the capability and process within the Department of Homeland Security developed under section 1705(c).

(g) PRESERVATION OF CONTRACTUAL OBLIGATIONS AND RIGHTS.—Nothing in this title shall be construed—

(1) to amend, repeal, or supersede any current or future contractual agreement, terms of service agreement, or other contractual relationship between any entities, or between any entity and a Federal entity; or

(2) to abrogate trade secret or intellectual property rights of any entity or Federal entity.

(h) ANTI-TASKING RESTRICTION.—Nothing in this title shall be construed to permit the Federal Government—

(1) to require an entity to provide information to the Federal Government;

(2) to condition the sharing of cyber threat indicators with an entity on such entity's provision of cyber threat indicators to the Federal Government; or

(3) to condition the award of any Federal grant, contract, or purchase on the provision of a cyber threat indicator to a Federal entity.

(i) NO LIABILITY FOR NON-PARTICIPATION.—Nothing in this title shall be construed to subject any entity to liability for choosing not to engage in the voluntary activities authorized in this title.

(j) USE AND RETENTION OF INFORMATION.—Nothing in this title shall be construed to authorize, or to modify any existing authority of, a department or agency of the Federal Government to retain or use any information shared under this title for any use other than permitted in this title.

(k) FEDERAL PREEMPTION.—

(1) IN GENERAL.—This title supersedes any statute or other provision of law of a State or political subdivision of a State that restricts or otherwise expressly regulates an activity authorized under this title.

(2) STATE LAW ENFORCEMENT.—Nothing in this title shall be construed to supersede any statute or other provision of law of a State or political subdivision of a State concerning the use of authorized law enforcement practices and procedures.

(l) REGULATORY AUTHORITY.—Nothing in this title shall be construed—

(1) to authorize the promulgation of any regulations not specifically authorized by this title;

(2) to establish or limit any regulatory authority not specifically established or limited under this title; or

(3) to authorize regulatory actions that would duplicate or conflict with regulatory requirements, mandatory standards, or related processes under another provision of Federal law.

(m) AUTHORITY OF SECRETARY OF DEFENSE TO RESPOND TO CYBER ATTACKS.—Nothing in this title shall be construed to limit the authority of the Secretary of Defense to develop, prepare, coordinate, or, when authorized by the President to do so, conduct a military cyber operation in response to a malicious cyber activity carried out against the United States or a United States person by a foreign government or an organization sponsored by a foreign government or a terrorist organization.

SEC. 1709. REPORT ON CYBERSECURITY THREATS.

(a) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this title, the Director of National Intelligence, in coordination with the heads of other appropriate elements of the intelligence community, shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches.

(b) CONTENTS.—The report required by subsection (a) shall include the following:

(1) An assessment of the current intelligence sharing and cooperation relationships of the United States with other countries regarding cybersecurity threats, including cyber attacks, theft, and data breaches, directed against the United States and which threaten the United States national security interests and economy and intellectual property, specifically identifying the relative utility of such relationships, which elements of the intelligence community participate in such relationships, and whether and how such relationships could be improved.

(2) A list and an assessment of the countries and nonstate actors that are the primary threats of carrying out a cybersecurity threat, including a cyber attack, theft, or data breach, against the United States and which threaten the United States national security, economy, and intellectual property.

(3) A description of the extent to which the capabilities of the United States Government to respond to or prevent cybersecurity threats, including cyber attacks, theft, or data breaches, directed against the United States private sector are degraded by a delay in the prompt notification by private entities of such threats or cyber attacks, theft, and breaches.

(4) An assessment of additional technologies or capabilities that would enhance the ability of the United States to prevent and to respond to cybersecurity threats, including cyber attacks, theft, and data breaches.

(5) An assessment of any technologies or practices utilized by the private sector that could be rapidly fielded to assist the intelligence community in preventing and responding to cybersecurity threats.

(c) FORM OF REPORT.—The report required by subsection (a) shall be made available in classified and unclassified forms.

(d) INTELLIGENCE COMMUNITY DEFINED.—In this section, the term ''intelligence community'' has the meaning given that term in section 3 of the National Security Act of 1947 (50 U.S.C. 3003).

SEC. 1710. CONFORMING AMENDMENTS.

(a) PUBLIC INFORMATION.—Section 552(b) of title 5, United States Code, is amended—

(1) in paragraph (8), by striking ''or'' at the end;

(2) in paragraph (9), by striking ''wells.'' and inserting ''wells; or''; and

(3) by inserting after paragraph (9) the following:

''(10) information shared with or provided to the Federal Government pursuant to the Cybersecurity Information Sharing Act of 2015.''.

(b) MODIFICATION OF LIMITATION ON DISSEMINATION OF CERTAIN INFORMATION CONCERNING PENETRATIONS OF DEFENSE CONTRACTOR NETWORKS.—Section 941(c)(3) of the National Defense Authorization Act for Fiscal Year 2013 (Public Law 112–239; 10 U.S.C. 2224 note) is amended by inserting at the end the following: ''The Secretary may share such information with other Federal entities if such information consists of cyber threat indicators and defensive measures and such information is shared consistent with the policies and procedures promulgated by the Attorney General under section 1705 of the Cybersecurity Information Sharing Act of 2015.''.

SEC. 1711. CRIMINAL BACKGROUND CHECKS OF EMPLOYEES OF THE MILITARY CHILD CARE SYSTEM AND PROVIDERS OF CHILD CARE SERVICES AND YOUTH PROGRAM SERVICES FOR MILITARY DEPENDENTS.

(a) EMPLOYEES OF MILITARY CHILD CARE SYSTEM.—Section 1792 of title 10, United States Code, is amended—

(1) by redesignating subsection (d) as subsection (e); and

(2) by inserting after subsection (c) the following new subsection (d):

''(d) CRIMINAL BACKGROUND CHECK.—The criminal background check of child care employees under this section that is required pursuant to section 231 of the Crime Control Act of 1990 (42 U.S.C. 13041) shall be conducted pursuant to regulations prescribed by the Secretary of Defense in accordance with the provisions of section 658H of the Child Care and Development Block Grant Act of 1990 (42 U.S.C. 9858f).''.

(b) PROVIDERS OF CHILD CARE SERVICES AND YOUTH PROGRAM SERVICES.—Section 1798 of such title is amended—

(1) by redesignating subsection (c) as subsection (d); and

(2) by inserting after subsection (b) the following new subsection (c):

''(c) CRIMINAL BACKGROUND CHECK.—A provider of child care services or youth program services may not provide such services under this section unless such provider complies with the requirements for criminal background checks under section 658H of the Child Care and Development Block Grant Act of 1990 (42 U.S.C. 9858f) for the State in which such services are provided.''.

(c) FUNDING.—Amounts for activities required by reason of the amendments made by this section during fiscal year 2016 shall be derived from amounts otherwise authorized to be appropriated for fiscal year 2016 by section 301 and available for operation and maintenance for the Yellow Ribbon Reintegration Program as specified in the funding tables in section 4301.

The PRESIDING OFFICER. Amendment No. 1921 is rendered moot.

The Senator from Texas.

Mr. REED addressed the Chair.

Mr. CORNYN. Mr. President, regular order.

Mr. REED. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The Senator from Texas.

Mr. CORNYN. Mr. President, turning to the underlying legislation that we are debating, the Defense authorization bill, I can't think of anything more basic or fundamental to the Federal Government's responsibility than national security and defense and to make sure we provide our men and women in uniform with the resources they need in order to do the job they volunteered to do on our behalf. Of course, many of us have commented time and again on this floor and elsewhere about the increasing complexity of the threats facing our national security and the security and peace of the world.

This legislation enables our troops to get the funding and the resources and the authorities they need in order to have success on the battlefield. As we consider the current state of the world, it is clear why this bill is vital. We live in a world marked by constant dynamic threats to our way of life. For example, parts of the Middle East and North Africa have been overrun by the Islamic State, and the region continues to be a hotbed of failed states and ungoverned places. If we have learned anything from 9/11, it is that ungoverned spaces are a threat to our national security, because that is where our adversaries will organize and train and then export those threats to our homeland.

Despite ongoing negotiations, Iran remains an enemy of the United States and continues its campaign to achieve regional domination and become a threshold nuclear State, threatening our most trusted allies and partners in the region. In Europe and in Asia, Russia and China continue to threaten our allies in their respective neighborhoods, using a growing array of soft-power and hard-power tactics to twist arms and to coerce our friends and allies. These new dynamic threats include cyber attacks, which have been much in the news today, including espionage and just outright theft of our intellectual property in seed corn created from the brains and ingenuity of American entrepreneurs and creators. Today, our courageous men and women in uniform are tasked with the challenge of facing these many threats and many others in regions all around the world.

So it is astounding to me that the Democratic leader, in the face of these threats and in the face of our grave responsibilities to meet these challenges, would come to the floor and suggest that debating this bill would be what he called a ''waste of time'' and go further to say that the Democratic minority would consider filibustering this legislation. It is just unbelievable.

This blatant disregard for our responsibilities and for our troops is very troubling, particularly because this bill has historically been one that has enjoyed broad bipartisan support. In fact, as our colleague, the senior Senator from Arizona, pointed out in an op-ed he wrote yesterday, Congress has passed a Defense authorization bill for 53 consecutive years—53 consecutive years—because it is a national priority. It should be, and it is. Up to now, this bill has been marked by strong bipartisan backing in the committee. The bill sailed through the Senate Armed Services Committee with a bipartisan vote of 22 to 4. We don't get much more bipartisan in today's Senate than that.

Yet, with all of the support from both sides of the aisle and even with such a clearly demonstrated need as the funding and well-being of our troops and their families, the President himself—the Commander in Chief—has threatened to veto this bill—a bill that actually provides the full funding levels he himself requested.

It is important to note—because some of our colleagues on the other side have said that the problem with this bill is that it doesn't spend enough money or that we ought to reallocate our nondefense discretionary spending to increase that, as well—that this bill includes the exact same level of funding that President Obama himself requested in his budget. So why in the world would the President threaten to veto a bill that meets the funding levels that he himself identified in his budget?

For some reason, instead of focusing on our most fundamental responsibilities of funding the brave men and women in our Armed Forces and making sure they have the resources they need to keep our country safe, our Commander in Chief and the minority leader are threatening to hold this bill hostage to extract more government spending for nondefense discretionary spending for organizations and agencies such as the Internal Revenue Service. So why in the world would we hold national security spending hostage so we can spend more money on the IRS? It is just a complete upside-down view of our priorities.

So the President's lack of strategic depth or his understanding of our Nation's most fundamental duties is really astounding. I am troubled to say this, but I think it is actually true: I think the President understands our Nation's fundamental duties very clearly. The problem is that this threat to hold this bill hostage is just cynical. It just uses a political tool to try to gain advantage when it comes to raising the caps on nondefense discretionary spending. For a President who admits that he doesn't have a complete strategy to defeat the Islamic State, I find his comments to be irresponsible. He is threatening to veto this bill to satisfy the far leftwing of his party, which doesn't believe government could ever spend too much money and that government is ever big enough. The government is never big enough or spends enough for some of our colleagues across the aisle and some of the political base in the President's party.

Just this morning, the Washington Post reported that Senate Democrats have now come up with a brand-new political strategy, and this time they are going further—to threaten to block all funding bills for the rest of the summer, including the Defense appropriations bill, which I know the majority leader is scheduling to be debated and voted on right after we complete our work on this legislation. As a matter of fact, the Democratic leader said this morning: ''We're headed for another shutdown.'' Senator REID said: ''They did it once, they're going to do it again. . . . They want to wait until the fiscal year ends and then close up government.''

It is bad enough that Democrats are threatening to filibuster the defense spending bill, but now they are claiming that it is really the Republicans' fault. In other words, they are saying: We are not for stopping the Defense authorization bill.

We are for funding our national responsibilities when it comes to national security. But because our Democratic friends wish to hold the Defense authorization bill and the Defense appropriations bill hostage, they somehow now are claiming that we are the ones responsible. Because we won't accede to their insatiable demand for bigger government and more government spending, and we won't allow them to hold our troops and their families and our national security hostage, we are the ones at fault.

But, today, as we know, thanks to the Washington Post, the filibustering of this and other bills is just part of a political strategy.

One point I have to acknowledge is the candor of our colleagues on the other side of the aisle. If we want to know what they are planning to do, all we have to do is read the newspaper, because they are more than happy to tell us exactly what they are going to do and what their plans are.

This is all part of a cynical political strategy to keep the Senate from working and to deny funding to our Armed Forces while bulking up Federal agencies such as the Environmental Protection Agency and the IRS. This is shameless, and it is hypothetical, and the American people will not be fooled by it.

I wish to remind our colleagues across the aisle that stifling debate and blocking votes is a pretty lousy political strategy, as well. It is what lost them control of this Chamber last November. It is a losing strategy, it is bad policy, it is cynical politics, and the American people understand that. It is simply shameful that they are trying to use our troops, who protect this great Nation, as some sort of leverage in some sort of political game.

I don't have to remind the Presiding Officer, who continues to serve honorably in our military services, that we live in a very dangerous world. Somehow, we don't pay enough attention to that until something reaches out and bites us or injures someone we love. Our Armed Forces face new and growing threats on a daily basis. Our troops deserve our full attention and every resource they need as they serve and defend our country around the world.

So that is why I have come to the floor, to say: Why in the world, after 53 consecutive Defense authorization bills, would the Democratic leader—and indeed with the complicity of the President of the United States himself—say they are going to hold this Defense bill hostage until they get what they want when it comes to spending more money?

This bipartisan bill, which focuses squarely on the needs of our warfighters and authorizes funding at the same level the President himself suggested, should not be held hostage to political gamesmanship. So I would encourage the more sensible Members across the aisle to focus on the troops and their families, not on the partisan agenda of their leadership, and pass this legislation to provide the funding our troops need to continue to do their courageous work of keeping our country safe.

One way my colleagues could play a constructive role and move this legislation forward, instead of threatening to filibuster, is to work with us on commonsense amendments, such as the one I have filed that is pending on the underlying bill.

Under current law, the President has discretion to allow energy exports to vulnerable allies, our partners in Europe, and around the world when it is deemed to be in our national interest. The amendment I have offered in the underlying bill simply reaffirms the existing authority of the President of the United States but encourages the President not to allow our adversaries, such as Vladimir Putin, to use energy supplies for vulnerable countries in Europe as a weapon. It would also commission a report that would allow us to get an accurate assessment of just how dependent our allies in the region are on those who would wield their energy supply as a weapon.

This amendment is a commonsense measure that serves as a first step to addressing the requests—the pleas in some cases—of our allies and partners in an increasingly unpredictable world, and it doesn't change the existing authority the President already has.

I would urge our colleagues to put down the political playbook and work with us in a constructive way on the underlying legislation. This has been the great tradition of the Defense authorization bill and one that is being threatened by the political gamesmanship that we see threatened by the Democratic leader and, indeed, even with the complicity and the fingerprints of the President of the United States.

We owe it and so much more to our troops, who are relying on us to act today. Even more than that, we have a duty to the country to make sure we maintain the security of the American people.

I yield the floor.

Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mrs. FEINSTEIN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

CYBERSECURITY INFORMATION SHARING ACT

Mrs. FEINSTEIN. Mr. President, last week we learned of the latest in the string of massive breaches of private information from cyber penetrations, this time of government personnel records held by the Office of Personnel Management.

In its annual worldwide threat assessment, the intelligence community this year ranked cyber intrusions and attacks as the No. 1 threat to our Nation's security. Cyber attacks and threats are also a major drag on our economy, with the theft of billions and billions of dollars of intellectual property and actual money from our Nation's businesses. Quite simply, cyber attacks are a major and growing threat to every aspect of our life.

It is with that background that Senator BURR and I began working early this year on a new cyber security information-sharing bill. It is a first-step bill, in that for sharing company to company or sharing cyber threat information directly with the government, a company would receive liability protection and therefore feel free to have this kind of constructive interchange.

The Senate Select Intelligence Committee produced the bill in the last Congress, but it didn't receive a vote. Chairman BURR and I have been determined not only to get a vote but to get a bill signed into law. It should be evident to everybody that the only way we will get this done is if it is bipartisan.

With significant compromises on both sides, we put together the Cybersecurity Information Sharing Act, a bill approved in March by our Intelligence Committee by an overwhelming 14-to-1 vote. That bill has been ready for Senate consideration for nearly 3 months but has not yet been brought to the floor.

Last week's attack underscores why such legislation is necessary.

The Democratic leader told me many weeks ago that this issue is too important for political wrangling, that he would not seek to block or slow down consideration of the bill and would work to move the bill quickly. So the bill is ready for floor consideration.

Now, a number of my colleagues would like to propose amendments—as is their right—and I expect I would support some of them and would oppose some of them. The Senate should have an opportunity to fully consider the bill and to receive the input of other committees with jurisdiction in this area. Unless we do this, we won't have a bipartisan vote, I believe, because, like it or not, no matter how simple—and I have been through two bills now—this was not an easy bill to draft because there are conflicts on both sides.

Filing the cyber security bill as an amendment to the Defense authorization bill prompted a lot of legitimate and understandable concern from both sides of the aisle. People want debate on the legislation, and they want an opportunity to offer relevant amendments. To do this as an amendment—when Senator BURR discussed it with me, I indicated I did not want to go on and make that proposal—I think is a mistake.

I very much hope that the majority leader will reconsider this path, and that once we have finished with the Defense authorization bill, the Senate can take up, consider, and hopefully approve the cyber security legislation. I think if we do it any other way, we are in for real trouble, and this is the product of experience. So I very much hope that there can be a change in procedure and that this bill—I know our leader will agree—could come up directly following the Defense authorization bill.

I thank the Chair, and I yield the floor.

Mrs. FEINSTEIN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. COTTON. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Is there objection?

Mrs. FEINSTEIN. I object.

The PRESIDING OFFICER. Objection is heard.

The clerk will continue to call the roll.

The legislative clerk continued with the call of the roll.

Mr. COTTON. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. COTTON. Mr. President, I speak today about Cotton amendment No. 1605, addressing funding for the National Nuclear Security Administration, the administration that safeguards our nuclear stockpile for the country. The Obama administration, in its budget earlier this year, requested approximately $50 million per year for the next 5 years for the administration to be able to dismantle old or obsolete warheads. My amendment would simply codify President Obama's own budget request, limiting the administration to spend $50 million per year for the next 5 years on nuclear dismantlement.

My amendment also includes a waiver that would allow the President to increase the amount of spending under certain limited conditions. This amendment has been approved not only by the majority but also the minority of the Armed Services Committee.

I offer this amendment because of troubling statements from the Obama administration about their intent to accelerate nuclear disarmament, however. Last month, Secretary of State Kerry announced at the Nuclear Nonproliferation Review Conference that the United States would accelerate its dismantlement of nuclear warheads by 20 percent. Beyond obsolete or outdated warheads, I do not believe that is a priority. Nuclear modernization is a priority.

We should not be accelerating our nuclear disarmament by up to 20 percent because it would send the exact wrong message to Russia, other adversaries, and our allies. Russia is making overt nuclear threats to the United States and our allies, and we are going to accelerate our unilateral nuclear disarmament? That defies logic.

Madam President, I ask unanimous consent to set aside the pending amendment in order to call up Cotton amendment No. 1605.

The PRESIDING OFFICER (Mrs. ERNST). Is there objection?

Mrs. FEINSTEIN. Madam President, reserving the right to object. I am very concerned about this. It unnecessarily limits the National Nuclear Security Administration's ability to dismantle the retired nuclear weapons that no longer have any role in our national defense.

The President's budget proposed $48 million for dismantlement, and this amendment would freeze funding at that level and at specific funding levels for the next 5 years. However, the Appropriations Committee, just last month, provided an additional $4 million for dismantlement in the Energy and Water bill.

I am ranking member on that committee. It was approved on a bipartisan basis, 26 to 4. This funding is appropriate and it is justified. The fact is, there are currently approximately 2,400 retired warheads awaiting dismantlement. The rate at which we dismantle these warheads does not have anything to do with the 4,800 warheads that remain in the stockpile, consistent with the New START treaty.

This is a treaty, not an agreement. The administration has committed accelerating dismantlement and we should support its goals of eliminating redundant nuclear weapons. I see no reason to imply congressional disapproval for this effort and to micromanage NNSA's weapons activity. Modernization and dismantlement go hand in hand. NNSA routinely shifts employees from weapons stockpile stewardship and modernization work to dismantlement to keep the workforce fully and usefully engaged. It is completely unnecessary to complicate this process. I object.

The PRESIDING OFFICER. Objection is heard.

Mr. COTTON. Madam President, I understand that the Senator from California objects to my amendment. But this is the Senate. This is an important issue. We should be debating the matter. If the Senator from California wishes to defeat my amendment, we should call it up and make it pending and have a vote on it, not object to an amendment simply being brought to the floor to be debated.

Is there a reason to manage our nuclear policy? Yes, I would say there is a strong reason. On many issues, the administration has shown itself less than forthcoming in dealing with Congress, in particular on nuclear policy. As we now know, the administration minimized reports of Russia's activities under the Intermediate Nuclear Forces Treaty at a time they were trying to pass the New START treaty in 2010.

I would further say this amendment simply codifies the President's budget request. The Senator from California said $48 million for this year. For the next 4 years after that, it is $48.3 million, $50 million, $52.4 million, $51.8 million. I will concede that, in sum, that is $50.1 million per year, on average. So I am giving the administration a haircut of $100,000 per year. If that is objectionable, I would be happy to modify my amendment to put it at $50.1 million per year.

But this Congress should not give the President a blank check to engage in further unilateral nuclear disarmament at a time when Vladimir Putin is making nuclear threats against the United States, invading sovereign countries, and his missiles are shooting civilian aircraft out of the sky in the heart of Europe.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. SESSIONS. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. SESSIONS. Madam President, I rise to speak on my amendment No. 1706. This amendment addresses the contributions of the member states to the North Atlantic Treaty Organization, in relation to their commitment towards their defense budgets within their economy.

At the 2006 NATO summit in Riga, Latvia, which I was honored to be able to attend, NATO member countries committed to spend a minimum of 2 percent of their national income, GDP, on defense. Furthermore, at the 2014 NATO summit in Wales, NATO member countries agreed again that ''allies currently meeting the NATO guideline to spend a minimum of 2 percent of their gross domestic product on defense will aim to continue to do so''.

They went on to state that ''allies whose current proportion of GDP spent on defense is below this level will: halt any decline in defense expenditure; aim to increase defense expenditure in real terms as GDP grows; aim to move towards the 2 percent guideline within a decade with a view to meeting their NATO Capability Targets and filling NATO's capability shortfall.''

Well, I suggest that is a pretty weak commitment, but it remains a commitment. It certainly can be stretched out, and they are already failing too often to meet those commitments.

So, in 2015, only 4 this year—only 4 out of the 28 NATO-member countries, including the United States, meet the 2-percent target. That is 4 out of the 28.

Regrettably, European NATO allies averaged just 1.33 percent of their GDP on defense, even though NATO countries have made numerous, unbinding, unfulfilled agreements to spend 2 percent. The United States currently spends 3.8 percent of its GDP on defense—a large portion of it defending Europe.

So, in contrast, the Organisation for Economic Co-operation and Development data shows that European-NATO allies averaged 24 percent of their GDP on social welfare programs, contrasting to 19 percent in the United States. So they spend more in-country on their programs while we are spending more to defend them.

Unfortunately, reductions in military spending are a common theme across Europe. Just 5 years ago, according to the NATO figures, France's military budget amounted to 2.4 percent of GDP. This past year, it stood at 1.9 percent, and France's budget law orders no increases before 2019. As for Germany, Europe's economic powerhouse, it spends only 1.3 percent of its GDP on defense. By the way, the European economy, as a whole, is as large or slightly larger than the U.S. economy as a whole.

So in 1990, NATO's European member states spent, on average, about 2.3 percent GDP on defense—well above today's average of 1.3. America's share of NATO military expenditures—get this, colleagues—is 75 percent. The U.S. share of the NATO military expenditures is 75 percent and has grown an additional 5 percent since 2007. This is a rather dramatic figure.

I had the privilege to be able to travel to Eastern Europe recently, and it was raised to us, by individuals in those countries, that they were somewhat embarrassed about this. But the reality is, they are taking no substantial steps to deal with it.

Former Secretary of Defense Robert Gates—who is one of the most wise people in the world, I believe, in terms of U.S. policy and international policy, served in multiple administrations over the years in the White House and as Secretary of Defense under President Obama and President Bush—in his last speech as Secretary of Defense had the following to say on this matter:

> Indeed, if current trends in the decline of European defense capabilities are not halted and reversed, future U.S. political leaders—those for whom the Cold War was not the formative experience that it was for me—may not consider the return on America's investment in NATO worth the cost.
>
> What I've sketched out is the real possibility for a dim, if not dismal future for the transatlantic alliance. Such a future is possible, but it is not inevitable. The good news is that the members of NATO—individually and collectively—have it well within their means to halt and reverse these trends, and instead produce a very different future.

This was his last speech. He made a speech on a subject he considered to be extraordinarily important. It is a statement he has made previously at other times, but it reflected, I think, something akin to Washington's Farewell Address as he raised and discussed one of the most important problems facing the world today; that is, the developed world, other than the United States, is not conducting itself financially in an effective way to defend themselves.

Former Secretary of State Henry Kissinger, for decades one of the world's wisest world leaders and commentators, has repeatedly questioned Europe's will. It gets down to that level: To what extent is Europe willing to pay a modest price to maintain their security?

There was a book out a number of years ago, referred to as ''Of Paradise and Power,'' and Robert Kagan's book notes that the Europeans are living in the paradise provided by American power.

So when the Russians took this aggressive step to invade the Ukraine, a nation we have considered for admission into NATO, took Crimea and otherwise acted in violation of international law, we announced a European reassurance initiative, $1 billion. This $1 billion was to be utilized in a way that would reassure our allies and reaffirm our commitment to Europe, even in the face of this dangerous and provocative action by Russia.

Well, colleagues, after having been to Europe and Eastern Europe on a number of occasions, I would say I am getting to the point where I want to be reassured. I want to have confidence in Europe's commitments.

At this volatile time in world history, this lack of commitment on the part of our European allies must end. We need to ensure that NATO members are spending at least what is needed and certainly the minimum 2 percent of GDP they repeatedly committed to spend.

The dangers in this world are much closer to Europe than they are to the United States, and our European allies are right to be concerned. They are anxious to have our presence. The requests for more and numerous military support, action from the United States, are even urgent in some of those countries. They want us there.

But, great danger arises from Europe living in an unreal comfort zone, living in the paradise of American power. Unless the history of the world has been dramatically altered, and it has not, threats to Europe will remain. Who will resist the dangerous pressures on Europe? Will our European partners just rest on American power? That is what the reality suggests is, in fact, occurring now.

Europeans now insist Greece must take painful financial steps for the good of the European Union to be a good team player, they say.

I think it is right and appropriate for the United States to call on our NATO

allies to do their part for this great alliance that has done so much for stability, prosperity, and peace for Europe and for the entire world.

This amendment before the Senate has overwhelming support, I believe. I think it will be accepted as part of the managers' package. The call it makes on NATO members is the absolute minimum, I think, that can be expected of them.

Let's consider the plain facts. The deployment of U.S. military forces to any nation in the world, for the purpose of defending that nation and a region, is an august thing. Obviously, the military might of the United States is unsurpassed. The United States cannot and must not take these commitments lightly. The ramifications of our commitment to the defense of a foreign nation are significant—grave indeed.

This Nation has every right and a duty to our citizens to ensure that those with whom we partner do their share. The idea that a small nation can simply send an email to the United States calling for more forces whenever they become nervous—while taking only limited steps to fund and defend their own country—suggests a disconnect with reality.

This Senate, by this amendment, is sending a clear call for NATO to do more. It is not too late to maintain this alliance as the force for good it has always been. But everyone on both sides of the Atlantic who understands these issues realizes we are in a precarious situation if a miscalculation occurs, and miscalculations can lead to violence and war.

So it is time to make clear the strength of our commitment to each other and to ensure there is no miscalculation. To do that, more is required of our NATO allies.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. VITTER. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

AMENDMENT NO. 1473

Mr. VITTER. Madam President, I rise to speak about amendment No. 1473 that is pending. I will be modifying it, not now but later today, in a technical way. The majority and the minority have been notified of this modification, so I will be making that later, and I am going to talk about the substance of the amendment.

This amendment is very significant in terms of our Army force structure. It would limit any additional reductions the Army can make to Army BCTs, which have already been drastically reduced from 48 brigade combat teams in 2008 to 45 in 2013, to now 33 in 2015—so in just 7 years, from 48 to 33. Obviously, it was a dramatic reduction.

This is important because brigade combat teams are a very significant element of Army force structure, and many experts all across the spectrum would acknowledge that and would acknowledge that further significant reductions would be very dangerous.

To clarify, my amendment would require the Army to trim its force structure. It doesn't stop that trend, but it also offers protections for that primary core unit of the brigade combat team without mandating additional money, additional requirements, et cetera. There is a serious and urgent need for Congress to act quickly so the Defense Department has the authority and support it needs to defend our Nation.

This specific amendment protecting those core, required brigade combat teams is supported by the National Guard Association of the United States and the Association of the United States Army, the two key national groups that support the direct Army and the National Guard.

Some Members may argue that we don't want to micromanage the Army and how it deals with force structure. I certainly agree with that generally, but this is certainly not getting into the fine weeds. This is a major issue, and brigade combat teams are a major tool of their force structure. Furthermore, exactly this sort of limitation has been done in this bill, in the underlying bill, both with regard to the Air Force and with regard to the Navy.

The bill, as it stands on the floor coming out of committee, includes numerous provisions to block the elimination of certain weapons systems, such as the Air Force fighter inventory, the A–10, EC–130 Compass Call aircraft. So it is very similar on the Air Force side to justify blocking these eliminations. The chairman's report states:

> The committee believes further reductions in fighter force capacity, in light of ongoing and anticipated operations in Iraq and Syria against the Islamic State of Iraq and Levant, coupled with a potential delay of force withdrawals from Afghanistan, poses excessive risk to the Air Force's ability to execute the National Defense Strategy, causes remaining fighter squadrons to deploy more frequently, and drives even lower readiness rates across the combat air forces.

Exactly that same sort of rationale which is in the bill with regard to limitations of what the Air Force can do also applies to the Army and brigade combat teams.

In addition, the same sort of thing is already in this underlying bill with regard to the Navy. There is specific language blocking certain further reductions of aircraft carriers—again, a major element of force structure; again, Congress saying: No, don't go below this number. That is not justified. That will weaken our overall capability, and that will weaken force structure.

So again on the Navy side on this bill the chairman and the committee have done exactly the same thing. My amendment would simply do something very similar and equally as important and justified on the Army side with regard to brigade combat teams.

Because of the significance of brigade combat teams to Army readiness and operations, because of the enormous cuts that have already been made in those numbers in the last 7 years—from 48 to 33—I urge all of my colleagues, Democrats and Republicans, to support this commonsense amendment.

Again, Madam President, to underscore, I will be returning to the floor sometime today to modify my amendment in a technical way. Everyone—certainly including the majority and minority leaders on this bill—has been given those modifications. They are not controversial. I will simply wait for them to be on the floor to make that modification, which is within my right and purview and does not require unanimous consent, and then I am very hopeful this amendment will be teed up in the next group of votes, perhaps around 3:30.

Madam President, with that, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. MCCAIN. Madam President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

AMENDMENT NO. 1921

Mr. MCCAIN. Madam President, I want to say a few words about the Burr amendment, No. 1921, which has now been made pending. I am thankful for the leadership of Chairman BURR and Vice Chairman FEINSTEIN.

The language of this amendment, of which I am an original cosponsor, was overwhelmingly approved by a 14-to-1 vote in the Senate Select Committee on Intelligence in March.

Implementing legislation to address a long list of cyber threats that have become all too common is among my highest priorities. Earlier this month, it was the Office of Personnel Management and the Army. A few weeks before that, it was the Pentagon network, the White House, and the State Department. Before that, it was Anthem and Sony. That is just to name a few.

I am pleased we are able to consider this amendment on the National Defense Authorization Act. This voluntary information sharing is critical to addressing these threats and ensuring that mechanisms are in place to identify those responsible for costly and crippling cyber attacks and ultimately deterring future attacks.

Our current defenses are inadequate, and our overall cyber strategy has failed to deter cyber adversaries from continued attacks of intellectual property theft and cyber espionage against the U.S. Government and American companies. This failure to develop a meaningful cyber deterrent strategy has increased the resolve of our adversaries and will continue to do so at a growing risk to our national security

until we demonstrate that the consequences of exploiting the United States through cyber greatly outweigh any perceived benefit.

This amendment is a crucial piece of that overall deterrent strategy, and it is long past time that Congress move forward on information-sharing legislation. This legislation—again, 14 to 1 from the Select Committee on Intelligence—complements a number of critical cyber provisions which are already in the bill which will ensure that the Department of Defense has the capabilities it needs to deter aggression, defend our national security interests, and, when called upon, defeat our adversaries in cyber space.

The bill authorizes the Secretary of Defense to develop, prepare, coordinate, and, when authorized by the President, conduct a military cyber operation in response to malicious cyber activity carried out against the United States or a U.S. person by a foreign power.

The bill includes a provision requiring the Secretary of Defense to conduct biennial exercises on responding to cyber attacks against critical infrastructure. It limits $10 million in funds available to the Department of Defense to provide support services to the Executive Office of the President until the President submits the integrated policy to deter adversaries in cyber space, which was required by the National Defense Authorization Act for Fiscal Year 2014.

It authorizes $200 million for a directed evaluation by the Secretary of Defense of the cyber vulnerabilities of every major DOD weapons system by not later than December 31, 2019.

It requires an independent panel on DOD war games to assess the ability of the national mission forces of the U.S. Cyber Command to reliably prevent or block large-scale attacks on the United States by foreign powers with capabilities comparable to those expected of China, Iran, North Korea, and Russia in years 2020 and 2025.

It establishes a $75 million cyber operations procurement fund for the commander of U.S. Cyber Command to exercise limited acquisition authorities.

It directs the Secretary of Defense to designate Department of Defense entities to be responsible for the acquisition of critical cyber capabilities.

The cyber security bill was passed through the Select Committee on Intelligence because that is clearly, in many respects, among the responsibilities of the Select Committee on Intelligence. But I think it is obvious to anyone that the Department of Defense is a major player. I just outlined a number of the provisions of the bill which are directly overseen and related to the Department of Defense.

So my friends on the other side of the aisle seem to be all torqued-up about the fact that this cyber bill should be divorced from the Department of Defense. I know that my colleagues on the other side of the aisle are very aware that just in the last few days, 4 million Americans—4 million Americans—had their privacy compromised by a cyber attack. The Chairman of the Joint Chiefs of Staff has stated that we are ahead in every aspect of a potential adversary except for one, and that is cyber. There are great threats that are now literally to America's supremacy in space and to many other aspects of technology that have been developed throughout the world and are now part of our daily lives.

So I am not quite sure why my friends on the other side of the aisle should take such exception to legislation that addresses our national security and the threats to it, which literally every expert in America has agreed is a major threat to our ability to defend the Nation.

So I think there are colleagues who are not on the Intelligence Committee and are not familiar with the provisions of this bill. It clearly is not only Department of Defense-related, but it is Department of Defense-centric, with funds available to DOD to provide services to the Executive Office of the President, $200 million, cyber vulnerabilities of major DOD weapons system, an independent panel on DOD war games, and on and on. It is Department of Defense-related, and it is the whole purpose of the Defense authorization bill, which is to defend the Nation. To leave cyber security out of that—yes, there are some provisions in the underlying bill, but this hones and refines the requirements that we are badly in need of and gives the President of the United States and Secretary of Defense tools to try to limit the damage that is occurring as we speak.

I want to repeat—and to my colleague from Indiana who is a member of that committee, I would ask him—4 million Americans recently were compromised by cyber attack.

Mr. COATS. In response to my friend from Arizona——

Mr. MCCAIN. Madam President, I ask unanimous consent to engage in a colloquy with the Senator from Indiana.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. COATS. Madam President, this is a serious breach, and there is more to the story to be told. It shows the extreme position that we are in here as Americans, as there are those who want to take this country down, those who want to invade privacy of Americans and have the capabilities of breaching this. The legislation before us, and the reason why it is brought here now and, hopefully, will be attached to the Defense bill is that this needs to be done now and not later. How many breaches do we have to hear about—whether it is the private sector or whether it is the government sector—before this Congress and this Senate will stand up and say we have the capability of preventing some of these things from happening, but we need the legislative authority to do it. To delay and not even allow us to go forward with this puts more and more millions of Americans at risk, whether they work for the government or are in private industry.

Mr. MCCAIN. And isn't it true, I would ask my colleague from Indiana, that the Chairman of the Joint Chiefs of Staff recently stated that in the potential of our adversaries to threaten our security, we have a definite superiority in all areas except for one, which is in the issue of cyber security; is that correct?

Mr. COATS. I think that is obvious, because, clearly, while we have the capability to address some of these issues, we are not allowed to use the capability. This legislation gives us the opportunity to have a cooperative effort. Some of those who resist the use of this because they think it is potentially a breach of privacy now understand that breaches are occurring from outside and into the United States, by those who are enemies of the state, those who are criminal groups, those who are terrorist groups. While we may have the capacity to deal with this, without this legislative authority we are not allowed to use it.

So what an irony—what an irony that some are saying: We can't trust the government on this to help us. This is defense. This is like saying we can't trust the Department of Defense, we can't trust the Army or the Navy to protect us from attack because it is government-run. Now, they are saying there are some operations in government here that are part of our defenses that can't be used until we have authority. The irony is that people's privacies are being breached by all of these attempts, and we are denying the opportunity to put the tools in place to stop that from happening.

Mr. MCCAIN. Could I ask my colleague again: The 4 million people whose privacy was just breached—4 million Americans—what potential damage is that to those individual Americans?

Mr. COATS. Well, we are just learning what damage this is and how it can be misused in any number of ways. Some of this information is classified. But I can say to my colleague from Arizona, the chairman of the Armed Services Committee, that this puts some of our people and some of our systems in great peril. It is something that needs to be addressed now and not pushed down the line.

Mr. MCCAIN. So it seems to me that to those 4 million Americans, we owe them and it is our responsibility—in fact, our urgent responsibility—to try to prevent that same kind of breach from being perpetrated on 4 million or 8 million or 10 million more Americans. If they are capable of doing it once to 4 million Americans, what is to keep them from doing the same thing to millions of Americans more, if we sit here idly by and do nothing on the grounds that the objection is that it is not part of the Department of Defense

bill, which seems to me almost ludicrous?

Mr. COATS. Well, since the Department of Defense is one of those agencies being attacked, I would certainly think this is the appropriate attachment to a bill for which, hopefully, we will be given the opportunity by our friends across the aisle. Hopefully, we will be able to pass it in the Senate, move it on to the House, and get it to the President so that these authorities can be in place.

The Senator mentioned 4 million. A company whose headquarters is in the State of Indiana, Anthem insurance company, was breached—and this is public information—of 80 million people on their roles. That is almost one-third of all Americans who have had their private information breached by a cyber attack—not to mention the threat that comes from cyber attack on our critical infrastructure.

What if they take down the financial system of one of our major banks or several banks? What if they take down the financial transactions that they place on Wall Street every day? What if they shut down an electric power grid in the middle of February when the temperatures in the Northeast are in minus-Fahrenheit temperatures or when it is 110 degrees in Phoenix and you lose your power and can't turn on air conditioning? People will die. People will be severely impacted by this. To not go forward and give authorization to use the tools to try to better protect American safety is not only unreasonable but is a very serious thing.

Mr. MCCAIN. I thank my colleague from Indiana for his outstanding work on a very difficult issue that poses a threat to every American and citizens throughout the world.

I yield the floor.

The PRESIDING OFFICER (Mr. TILLIS). The Senator from Louisiana.

AMENDMENT NO. 1473

Mr. CASSIDY. Mr. President, I rise in support of Senator VITTER's amendment No. 1473, which requires the Army to maintain no fewer than 32 brigade combat teams, which are also referred to as BCTs.

I support this amendment because cutting the brigade combat teams is cutting the core of the Army's structure and their ability to perform their mission. This amendment requires the Army to maintain a brigade combat team level of 32. Currently, the Army is planning on cutting these to 30 and to continue cutting to a point where we will have a hollow force. This is a short-sighted approach to a bigger problem.

First, what the amendment says is that the Secretary shall give priority under this paragraph to be carried out as funding or appropriations become available.

Secondly, nothing in this section shall be construed to supersede the Army's manning of brigade combat teams at designated levels, and it requires congressional defense committees to have a report on the current manning of each brigade combat team of the Army. It also ensures that the Army National Guard brigade combat teams are maintained at 26, and this accounts for the deactivation of two Air National Guard brigade combat teams previously agreed to.

You may ask, Why do we need 32 brigade combat teams? At the height of the Iraq and Afghanistan wars, we had 48 brigade combat teams. If we have noticed, in the Middle East, it is getting worse, not better. This is not to say that we will commit these troops, but it will be to say that we shall maintain our readiness.

Next, the Army's key weapon system is the brigade combat team. This amendment protects that key weapon from those cuts.

Lastly, reducing brigade combat teams does not—I emphasize, does not—make existing brigade combat teams more ready. It wears them out. If you have fewer teams, they are deployed more often in whatever activity they are deployed to, and that stretches that manpower and womanpower potentially to the break.

Under this, with the higher level of force, there is less stress upon those who are there maintaining their readiness. In total, this amendment requires the Army to take a closer look at their strategy and risk, forcing the Army to think long term instead of just cutting the most crucial part of our force, which is the people, the human capital, our fellow citizens.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mr. PORTMAN. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. PORTMAN. Mr. President, I rise today to support the underlying bill we are talking about on the floor, which is the Defense authorization bill.

At a time of a rapidly deteriorating security environment around the world, we need to modify our policies. From the violence in Iraq and Syria to China's aggressive land reclamation in the South China Sea to Russia's activities on the eastern border of Ukraine as we speak here today—all of this is going on. We live in a world that is a lot less safe and less friendly to U.S. interests. Every day we see more of this. Frankly, it is time for us here in the Senate to help by changing some of our policy approaches to address this changing and more dangerous situation we see around the world.

I would hope we can do this on a bipartisan basis. Our differences with regard to other issues tend to be more pronounced, but with regard to national security, normally we come together. I am concerned with what I am hearing, at least from some of the debate I have heard on the floor, where it sounds as though some of our colleagues on the other side of the aisle would like to actually shut down this debate and not have a debate on some of these amendments and not have some votes on some of these amendments and not have a vote on this bill to try to adjust our national security posture so that we can address these new challenges around the world. It doesn't mean that everything that this side of the aisle wants to do would be accepted. Democrats would have the chance to offer their ideas, and we would have a good debate on it, and they would have a say in it. We need Democrat support to get the legislation done. But let's have that debate and that discussion.

So I hope that what I am hearing is not accurate. I hope we will be able to come together and continue this discussion and be able to have votes on amendments and on the final bill and then be able to help, to the extent we can in the Senate, to adjust our foreign policy and our national security policy to address these very real threats we see emerging all over the world.

I will give an example of one that I will offer today. This is an amendment that has to do with Ukraine. As some of my colleagues know, the situation in Ukraine has deteriorated significantly in the last year or so, and it has done so because Russia not only invaded Crimea and took that part of Ukraine but they are also now continuing their aggression on the border of Ukraine. This is a situation that affects us as Americans because Ukraine is our ally. Ukraine is a country that has decided to stand with us. It is time for us and the other NATO countries to stand with them.

Our policy toward Ukraine, in my view, has been not just insufficient but it has been kind of piecemeal. We haven't had a strategy to deal with this issue. So what this amendment attempts to do is to take the language that is in the underlying legislation—already in the bill the committee put together—and improve it so that, indeed, we do have a more comprehensive strategy toward Ukraine. This is incredibly important not just for Ukraine but for the international order, for our national security, and for our ability to help stop this aggression in Europe—the first, really, since World War II, where we have seen that a country is going across another country's boundaries and actually violating territorial integrity.

I visited Ukraine a couple of months ago in April. I got to see some of the conflict consequences firsthand. For those who have been to Ukraine—a number of my colleagues have, including Senator DURBIN, who just got back from Ukraine—I think they would all agree with me that Ukraine is in a state of war and it is under siege. That makes it much more difficult for Ukraine to do what they know they need to do, which is to improve their

economy, to deal with corruption, to have more transparency, to become more like those countries they want to emulate—the European countries and the United States of America. They are attempting to do that, but it is difficult when they have this conflict on their border where troops are being killed and civilians are being killed and where they have to devote enormous amounts of time and resources.

Just this week I had the opportunity to meet with the Prime Minister of Ukraine and the Finance Minister, both of whom are in town. In fact, we met with them yesterday as part of the Ukrainian Caucus, which I cofounded with Senator DURBIN. I will tell my colleagues that talking to them, it is very troubling to hear what is happening in their country right now.

As some of my colleagues know, there is supposed to be a cease-fire in place. It came from the second of what is called the Minsk agreement. Whatever semblance of credibility this Minsk cease-fire had left—I don't think it had much—it has now totally crumbled. Just last week, combined Russian-separatist forces launched a major assault to the north and southwest of the Province of Donetsk. Donetsk is one of those areas also known as an oblast or a province, where there is a lot of Russian and Russian-separatist activity. They were focused on this strategic town of Maryinka. We probably saw some of this on TV. It is very troubling that once again it looks as of these separatist forces, backed by Russia and Russian equipment, which are directly involved in this, are beginning to push back into Ukraine again.

The casualty reports are still coming in, but it appears that dozens have been killed or wounded in this assault, according BBC. These independent news organizations are following this, and I hope all of us are focused on this. The U.S. intelligence in the area is not what it ought to be, frankly, in my view, so we do need to rely on some of these media sources.

It is very clear that in terms of this assault, they were using tanks and heavy multiple-launch rocket systems and over 1,000 men were involved. So clearly, this is something that is not only a serious military exercise, but it is one that is backed by Russia, using Russian equipment. We have seen just how committed the Russian Government is to this—to promoting instability in that region of the world. They are committed.

The question is whether we are committed to step up and support the people of Ukraine. This is something that, in my view, the NATO forces and the United States should have done a long time ago—not by us getting involved directly, which, frankly, that is not what they are asking for. They are asking for assistance and aid to be able to defend themselves. They are asking for us to help them to be able to stop this assault by giving them just the basic weaponry they need to stop tanks, potentially to stop aircraft if aircraft get involved, and to be able to stop the invasion and to protect the territorial integrity of the country of Ukraine.

The President and some of his top advisers continue to stand in the way of meaningful U.S. and NATO action. They have told me they fear that it would provoke Russia, as if deadly clashes such as the one we saw last week and, in fact, yesterday—and we will continue to see today, probably, this steady stream of Russian tanks, artillery pieces, and soldiers into Ukraine—aren't evidence enough that NATO and American restraint has not deescalated this conflict. In fact, I think, in a way, it has emboldened the Russians, and it has inflamed them. Again, we are not talking about U.S. troops. What we are talking about is helping this country that is our ally that has turned to us through NATO, and we want them to be able to defend themselves.

The President continues to enforce this de facto embargo on any kind of significant weapon that Ukraine has said it needs to defend itself. He does that despite an overwhelming bipartisan consensus here in this body and in the House that it is time to increase this help. That would include lethal and nonlethal assistance to Ukraine. Congress has voted repeatedly to do just that, most notably in the Ukrainian Freedom Support Act, which was signed into law by President Obama in December. It also provided the President a national security waiver so he didn't have to do what we think he should do, which is to help them to defend themselves. The administration continues to withhold these arms, and it is time for that to end.

There is really very little disagreement on the capabilities that Ukraine needs. My amendment, which is amendment No. 1850, modifies and builds on the great work that Senator MCCAIN and Senator REED and others have already done in the bill. If we look at section 1251 of the bill, we will see that there is already assistance being provided to Ukraine, about $300 million. Our amendment directs the Secretary of Defense to spend this money in a way that all of us know is the appropriate way to ensure that we get the most bang for the buck and that we are giving them the assistance they really need.

It requires the Secretary of Defense to spend this money on a number of critical capabilities they need to defend themselves, including real-time intelligence, medium-range and long-range counter-artillery radars, defensive lethal assistance such as antitank weapons, UAVs, secure communications, and training to develop key combat, planning, and support capabilities at both the small unit level and at the brigade level. So it provides, frankly, less wiggle room for the administration by laying out exactly what is needed, what is being asked for by the Ukrainian military, and what, in this Chamber and having done a lot of work in this area through our Ukrainian Caucus and through other sources, we know is necessary.

Half of this $300 million under our amendment would be fenced off until at least $60 million of it is spent on the important capabilities the Ukrainians really need and have requested. That is the real-time intelligence, defensive lethal assistance, and counter-artillery batteries. If the administration fails to use this money for the purposes specified, then they have to use it to support other nations facing an increased risk of Russian aggression—countries such as Georgia and Moldova.

The amendment also requires DOD to report on the quantity and the type of security assistance being provided to Ukraine and how it complies with the purposes that are established in the legislation.

So the amendment helps to ensure that U.S. military assistance provides the assistance that will truly have a meaningful impact on the ground, and it gives Ukraine the tools it needs to defend itself.

It will also finally increase the cost of Russia's aggression. At no point has President Putin's decision to escalate this war been costly enough to force President Putin and the Russians to fundamentally reconsider their strategy. The annexation of Crimea, the campaign to destabilize and then invade eastern Ukraine last summer and fall, and the recent offensive have all happened despite a flurry of Western attempts to force a negotiated settlement. In fact, each temporary cease-fire in some senses has merely legitimized what the Russians have done. When there is this flurry of diplomatic activity, it tends to happen after the Russians have made gains on the ground and then it accepts those gains on the ground as the basis for negotiations, granting the separatists and their Russian supporters moral and, I would say, some legal equivalency that they simply don't deserve.

There is a pattern here. They seize the land, they preserve their gains through an internationally mediated cease-fire, and then they break that cease-fire, as they are doing right now, to seize more land and then use a new cease-fire to secure acceptance of their new gains. This has to stop.

The Obama administration and some EU members have been so fixated on ensuring that the successful implementation of the February cease-fire is a goal in and of itself that they have lost sight of this broader policy objective that a cease-fire should be working to achieve, which should be the defense of Ukrainian sovereignty and territorial integrity and support for the economic and political reforms that Ukraine needs. Let me underscore that. It is very difficult for them to undertake the economic and political reforms they need with this siege going on, and that is what we need. We need them to make those reforms so they cannot

just keep their territorial integrity but also so they become a stable, democratic, and prosperous country.

The Russian aggression in Ukraine is not going to go away or resolve itself simply because we wish it to. It will take a comprehensive strategy, which is laid out in this amendment, and coordinated political, military, and economic actions to change the current dynamic. Sanctions and economic assistance for Ukraine are important, but they are tools, not a strategy. Russian military action has been successful in threatening Ukraine's stability where other attempts to use economic or political means have failed. So what the Russians and separatists have found is that they have tried to disrupt through economic means and political means, and they haven't been successful there. In fact, the Ukrainians have rejected that, including by a recent election. It is no accident that their most successful tactic, the military tactic, is the one the United States and the West has done the least to address.

I have argued for months that this piecemeal, reactionary response to intimidation from Moscow is a recipe for failure. Instead, we have to have a comprehensive, proactive strategy that strengthens NATO, deters Russian aggression, and gives Ukraine the political, economic, and military support it needs to maintain its independence. We need a strategy that seeks to shape the outcomes, rather than one that is shaped by them. Much of that leadership must come from us and the administration here in the United States. Of course, this body has an important role to play, and that is what this amendment is all about.

Let's include funding for Ukrainian military assistance, not just in this authorization bill where we are setting the policy for it, but let's be sure in the spending bills that follow that we provide the Ukrainians what they need.

We should pass this legislation—the underlying bill—which Chairman MCCAIN has correctly noted is critical to helping us deal with so many challenges in the dangerous world we face. We should pass, again, the defense spending bill that doesn't leave the men and women in uniform without the means to carry out their incredibly important mission.

Importantly, for today's purposes, we have to be clear about what the stakes are in Ukraine. Events in Ukraine are a direct and deliberate challenge to the credibility of NATO itself, to the U.S.-led international order. President Putin's actions upend decades of established international norms and threaten the very foundation of this system order. Confidence in America and our European allies' unity and commitment to upholding this system deters bad actors. It incentivizes other countries to play by the rules. That is what we want. We want to help ensure peace, stability, and prosperity. If the credibility of our commitment is in doubt, the risk of economic collapse, more violence, and more instability increases. Into a void, chaos ensues. The Ukrainians understand this. They understand the importance of this conflict well beyond their borders. I hope in the United States of America we understand it. I hope we act in a way to help the Ukrainians be able to defend themselves and counter these activities on the eastern border of Ukraine.

Mr. President, I ask unanimous consent that the Senate be in a period of debate only until 3 p.m.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. PORTMAN. Mr. President, I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Mrs. BOXER. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mrs. BOXER. Thank you so much.

Mr. President, I ask unanimous consent to speak as in morning business until I conclude.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mrs. BOXER. Thank you very much, Mr. President.

HIGHWAY BILL

I come to talk about something different than the pending legislation—I have a number of things to say about that, a number of amendments I am supporting, many of them bipartisan.

At this point, I want to talk about the crisis we are facing in terms of our highway bill. We now have 51 days until the highway trust fund is empty. For all of us, this is a terrible prospect because a lot of our States rely on the Federal Government for up to 85 to 90 percent of their funding. Some States rely on less. My State relies on about 50 percent, but it is still huge. When this trust fund goes under, we are going to be in a lot of trouble.

What we have seen in this particular Senate since our Republican friends took over—and they are my friends—are a number of self-inflicted crises. Lord knows we have enough of them coming our way, we don't have to invent them—but we have seen several. In the first crisis we had, we were headed toward a partial shutdown of the Department of Homeland Security over an unrelated immigration issue. That was ridiculous. There was a lot of angst and finally it was resolved.

The second self-inflicted crisis ended last week, and it was brought about because the Republican leader didn't like the USA FREEDOM Act the House had passed overwhelmingly. As a result of his opposition, he, for several days, turned away from 57, 58, and more Senators who actually supported that bill, and he brought the surveillance of terrorists to a screeching halt. That wasn't what he wanted to do, but as a result of that self-inflicted crisis, we had a couple of moments there where we were dark. That problem luckily ended after a couple of days.

And now we are headed for another self-inflicted crisis, although I must say, from conversations I have had, I have some hope we can avert this crisis.

We have known about this since last December, when Democrats said: Let's stay in until we solve the highway trust fund. And Republicans said: Oh, no, let's just take care of it in May. Then, in May, the Republicans said: Let's just take care of it in July. That is no way to run a country. It is no way to run a transportation system. It is ridiculous, and our States, as I will point out later, are starting to cut way back on transportation projects—highways, bridges, and transit systems—because they are scared we are not going to reach agreement. So, 51 days, and I am here today to talk about it.

I want to show you a photograph of a bridge collapse in Minneapolis, MN, that happened in August of 2007. This bridge collapsed because there was a design flaw. It went undetected because there were not enough inspections made of the bridge because there wasn't enough being spent on ensuring that our bridges are safe.

To me, as I look at this, it is a metaphor for the current status of the highway trust fund, which supports thousands of businesses and millions of jobs and is on the verge of bankruptcy. You can see on this photograph the chaos, the danger, the disaster. Even though there are no people you can see, you can imagine the shock that occurred from this collapse.

Now, you might think this is an isolated incident, but I want to tell you we have 61,300 bridges in the United States which have been cited as being structurally deficient by engineers. The fact that we don't have a multiyear plan in place to fix these bridges is a shame upon our Nation. It is a shame upon our Nation. If you had your loved one in one of these cars, you would know this is unacceptable.

My message today to both sides of the aisle and to the House and the Senate is simple: We cannot afford to pass yet another short-term extension because that doesn't give us the certainty or the funds to fix bridges such as these—the 61,300 bridges that need repair. The continued inaction by Congress to enact a long-term bill is a disgrace and we need to meet this challenge head-on.

Now, I have heard rumors that we are making progress, and I know we are in the Environment and Public Works Committee. I serve on that committee with my friend Senator INHOFE. He and I have agreed we will go forward with a multiyear bill. This is wonderful. It is a little late in the day—we should have done it a long time ago—but I am proud he and I have agreed this is a priority. We have a date set of June 24 to mark up the bill. That is only about 35 days before the collapse of the trust

fund, but if all the other committees did their job as our committee did, we would be OK. So, yes, I am encouraged, but there are three other committees that haven't set up dates to mark up anything, as far as I know. Unless a miracle occurs, I believe my Republican friends are going to ask us for yet another short-term extension.

Now, if you went out on the street and stopped anybody—Republican, Democrat, whatever age—if you asked: Is it controversial for the Federal Government to fund transportation projects? They would say no.

Maintaining and improving our roads, bridges, and transit systems is a necessity. It is a necessary investment in our future that was recognized at our country's founding in the Constitution. That is why Senator INHOFE, who is one of the leading conservatives in the Senate, and myself, a very strong progressive Member, agree. Article I, section 8 of the Constitution gave Congress the authority ''to establish Post Offices and post Roads,'' and that has continued throughout our Nation's history.

Legislation authorizing Federal investment in our highways dates back 100 years to the passage of the Federal Aid Road Act of 1916 and the Federal Aid Highway Act of 1921.

I quote one of my favorite Presidents, Dwight Eisenhower. In 1956, he established the highway trust fund to serve as the major source of funding for our Nation's highway systems. This was significant because it was a large increase of Federal infrastructure investment. President Eisenhower knew we needed modern, efficient transportation systems to ensure our security. I say ''security'' because this is what President-elect Eisenhower said, a general and a hero from World War II: ''A network of modern roads is as necessary to defense as it is to our national economy and personal safety.''

He viewed a network of modern roads as a necessity to our defense. And I would add the word ''bridges,'' because you can have a convoy going over our bridges, too. So General Eisenhower and then President Eisenhower knew how important an efficient system of roads is to our military and national defense.

While serving in the Army way back in 1919, he joined a convoy of approximately 80 trucks and other military vehicles to cross from Washington, DC, to San Francisco to test the military's motor vehicles. This trip took 2 months, averaging 6 miles an hour. From this experience, plus his countless other experiences with the military, both home and abroad, he understood how important a reliable transportation system is to a First World nation.

Again, he said, ''A network of modern roads is as necessary to defense as it is to our national economy and our personal safety.''

Today, our economy still relies on interconnected transportation systems to move goods out of major ports of entry. I want to talk about my own State because at the Port of Los Angeles, we take in about 40 percent of the Nation's imports. We know they go straight out onto those roads and they deliver goods all over our great Nation.

We know there is a universal understanding that we have to maintain that road system so we can move people and goods efficiently. These surface transportation systems, which used to be the envy of the world, remain the foundation of a strong U.S. economy and enable us to compete in the global marketplace.

I hope you heard that I said our transportation system used to be the envy of the world because it is no longer the envy of the world. It is our fault. This has to be a priority. The United States lags behind its overseas competitors in infrastructure investment. According to the most recent World Economic Forum ranking within the past decade, the United States has fallen from 7th to 16th in the quality of our roads. We are behind countries such as China, Portugal, and Oman. This is ridiculous. The greatest Nation in the world—that is what we are—but we are falling behind on our infrastructure because we do not have the guts to face the fact that we have to fund the highway system.

Why are we behind? We only spend 2 percent of our gross domestic product on infrastructure, and that is a 50-percent decline from 1960. So we spend 2 percent of our gross domestic product while Europe spends 5 percent and China spends 9 percent.

The Federal Government does provide, as I said, over 50 percent of the capital expenditures for State highway projects nationwide, which means that all of our States and all of our local governments rely heavily on Federal funding to maintain and to improve their transportation. However, this is just a national average.

(Mr. SCOTT assumed the Chair.)

I see my colleagues have changed places here. For South Carolina, South Carolina depends on the Federal Government for 80 percent of their highway funds and their bridge repair—80 percent. California is 50 percent. North Dakota is 80 percent. Montana is 87 percent.

So what I am saying to my colleagues who I hope are somewhere listening is that if we do not act to fill the highway trust fund and to meet this looming made-up crisis—check out your State and how much you rely on Federal funds.

I already showed the picture of the Minnesota bridge collapse. I would like to put that up again because I think the Minnesota bridge collapse is a metaphor for where we are. Our whole thing is discombobulated. Our whole thing is disrupted because we do not have the courage to fund the highway trust fund, which, as President Eisenhower said all of those areas ago, is critical to our national security.

I am going keep this picture up here for a minute. I want to talk about our States and the bridges that are in disrepair. I hope people who may be listening across the country—if you live in one of these States, give a call to your Senator and ask him or her: What are you doing to fill the highway trust fund?

For example, in Kentucky there are over 1,100 structurally deficient bridges—bridges that could look like this. Pennsylvania has more than 5,000 structurally deficient bridges, which accounts for over 20 percent of all the bridges in their State.

In addition to the dangerously poor conditions of our bridges, 50 percent of our Nation's roads are in less than good condition. These roads and bridges that are no longer in good working condition span across the country.

So I am going to show a chart that I don't think we have ever talked about here. These are examples of deficient highway bridges in need of repair: Alabama, I–65 bridge over U.S. 11 in Jefferson County; Arizona, I–17 bridge over 19th Avenue in Maricopa County; Arkansas, I–30 bridge over the UP Railroad in Pulaski County; California, the Golden Gate Bridge, for goodness' sake; Colorado, the I–70 bridge in Denver; Connecticut, the West River Bridge in New Haven; District of Columbia, the Memorial Bridge. There was a press conference right near the Memorial Bridge by one of my colleagues a couple of weeks ago.

People are getting really scared about this. The point of this is not to scare anybody; the point of this is to say to my colleagues that we are responsible.

You know, maybe it is me. When I was growing up, my mother and father said: If you know there is a problem, do something about it. You don't have a right to turn your back and walk away.

I remember once when I was a county supervisor I found out that the county building we were in was earthquake-prone. Nobody talked about it. As soon as I found out it could collapse in an earthquake, I brought it to my colleagues. I said: Colleagues, we need to do something.

Do you know what they said, one or two of them? Don't bring it up. We don't have the money.

Excuse me. You have to have the money if you know the building you are in could collapse in an earthquake. You have to have some money if you know all of these bridges are in disrepair.

So let's continue. Florida, the Pensacola Bay Bridge; Georgia, a bridge in Fulton County; Hawaii, Halona Street Bridge in Honolulu; Illinois, Poplar Street Bridge; Indiana, the bridge over the CSX Railroad; Iowa, the Centennial Bridge; Kentucky—another one—the Brent Spence Bridge; Louisiana, another bridge there; Maine, the Piscataqua River Bridge; Maryland, the Chesapeake Bay Bridge; Massachusetts, the I–95 bridge in Middlesex; Michigan, the I–75 Rogue River Bridge.

Remember, if you are hearing my voice and you are hearing your State mentioned, give a call to your Senator and ask him or her, whether they are a Democrat or Republican, what they are doing about the highway trust fund because in 51 days it will go bust.

In Minnesota—did I mention that—the I–35 East Bridge over Pennsylvania Avenue; Mississippi, the Vicksburg Bridge; Missouri, the East Bridge over Conway Road; Nevada, the Virginia Street Bridge in Reno; New Hampshire, the I–293 bridge in Hillsborough; New Jersey, the Garden State Parkway in Union County; New Mexico, the Main Street Bridge; New York, the Brooklyn Bridge.

If you did not read the book ''The Great Bridge,'' you should read that book by David McCullough. It is an incredible book. That bridge was built so long ago. We don't want to lose the Brooklyn Bridge.

In North Carolina, the Greensboro Bridge; Ohio, the John Roebling Suspension Bridge; Oklahoma, the I–40 bridge over Crooked Oak Creek; Oregon, the Columbia River Crossing; Pennsylvania, the Benjamin Franklin Bridge; Rhode Island, the viaduct in Providence; South Carolina, the I–85 bridge in Greenville; Texas, the I–45 bridge over White Oak Bayou; Utah, the I–15 bridge over SR–93 in Davis County; Washington, the Evergreen Point Floating Bridge; Wisconsin, the U.S. 41 bridge over a river.

I just have to ask my friends on both sides of the aisle, if the roof on your house is about to cave in with your children inside and you know about it, would you find a way to pay for that repair or would you let it collapse on your kids? The answer is obvious. Of course you are going to fix the roof on your house. You have to keep infrastructure in good repair. The roof is caving in on our roads and our bridges. Lord help us if we do not act and someone else goes down in a crisis.

We can look at the details surrounding the I–35 bridge collapse in Minneapolis, MN, shown in that picture. On August 1, 2007, this eight-lane bridge, which is Minnesota's second busiest bridge, carrying 140,000 vehicles every day, suddenly collapsed during rush hour, killing 13 people and injuring 145 people.

It is critical that our Nation continue investing in our aging infrastructure. Everybody knows it. Everybody knows it—Congress, States, businesses, American workers. Republicans say they are for infrastructure investment, but they have not acted. Happily, we are having a markup—I am excited about it—in our EPW Committee. Not one other committee has marked up a long-term bill.

The highway trust fund is an integral part of how the Federal Government provides predictable, multiyear funding to States so that States can plan and construct long-term highway, bridge, and transit projects; therefore, the highway trust fund should be our No. 1 priority. In 51 days, the fund will go bust. It will be gone. We will not be able to pay all of our bills. So we have to move quickly because otherwise we will face a transportation shutdown.

The law that currently authorizes our transportation program is set to expire on July 31, and the highway trust fund will go bankrupt shortly thereafter. The clock is ticking, and failure is not an option. So let's put up that 51-day ticking time bomb, if you will. The highway trust fund is in serious trouble, and much needed transportation projects are in peril.

The short fund creates uncertainty, and uncertainty is terrible for business, it is terrible for workers, and it is terrible for the economy. Billions of dollars will be delayed to our States. Many States, including Utah, Arkansas, Georgia, Tennessee, and Wyoming, have already delayed or cancelled construction projects due to the uncertainty in the funding.

We are facing a crisis, and everybody knows it. If we do not act and act quickly, we will see a domino effect that will be felt throughout our economy.

I don't think I have to remind people that we came out of the worst recession since the Great Depression. I was here when we saw that happen at the end of George W. Bush's term. We were losing 700,000 jobs a month. I remember standing here on the floor of the Senate feeling that the whole world was collapsing around us.

The recovery is taking a long time, and thank God it is moving forward now. Our economy, though, is still recovering, and we must have a strong, modern, efficient transportation system to move goods and people. There are some people who absolutely need transportation to get to work. This is not a game. Either they need their cars or they need to hop on a bus or a subway. And we have 51 days until the highway trust fund will be empty.

The amount of money we need just to keep up with the demand right now to fix our roads and our bridges—that amount is $123 billion just to catch up on the nightmare we are facing. So we not only need a 6-year bill, but we need one that is robust so we can start spending some money on these repairs. Millions of jobs and thousands of businesses are at stake here.

You know, it is 51 days. And I have stood in several press conferences with business leaders, the chamber of commerce, the AFL–CIO, construction workers, the concrete people, the tar people, the granite people—you name it. They are united as one America in favor of a 6-year solution. I will show you just some of the people whom I have stood with over time in recent days: The AFL–CIO; the U.S. Chamber of Commerce—it is hard to get them on the same page, but they are on the same page and they want this fix; the U.S. Conference of Mayors; the American Association of State Highway and Transportation Officials; the American Council of Engineering Companies; the American Highway Users Alliance; the American Public Transportation Association; the American Road and Transportation Builders Association; the American Society of Civil Engineers; and the American Trucking Association.

The truckers have said to me: Senator, we are willing to pay more in our gas tax because we cannot continue to ride on these roads that are falling apart.

When was the last time someone came up to you and said ''Raise my gas tax''? It is rare. But the truckers have asked us to do it as long as we use the money to fix the road. The chamber of commerce has asked us to raise the gas tax 6 cents to 8 cents. I mean, this is unusual, and I know there is very little support for that.

I have proposed numerous ways to pay for the trust fund, including a refundable gas tax increase. So if you earn $100,000 or less in your family, you get back the tax increase, which is about $40 a year. So I think it is worth $40 a year to know that the bridge you drive on is safe, but we would make it refundable so that you would get that back if you are in the middle class or below.

I will tell you, facing a shutdown—and we are already seeing a shutdown in five, six, or seven States—is painful for businesses. I have had business people come before me with their heads in their hands because they do this work. They build the highways. They fix the bridges. They build the transit systems. And they know we have not come together yet. It is a recipe for disaster.

What planet are we living on? All of America wants this.

I will continue with some more of these names. I just read some of them; I will read some more: the Associated General Contractors; the Association of Equipment Manufacturers; the Association of Metropolitan Planning Organizations; the International Union of Operating Engineers; the Laborers' International Union of North America; the National Asphalt Pavement Association; the National Association of Counties; the National Association of Manufacturers.

The National Association of Manufacturers, the Associated General Contractors, the International Union of Operating Engineers, the Laborers' International Union of North America—this is all of America. This isn't red. This isn't blue. This is everybody. Everybody wants us to fix the roads. Everybody wants us to fix the bridges.

We have the National Association of Truck Stop Operators; the National Governors Association—the Governors are Republicans and Democrats, and they are begging us to get our act in gear and get this done; the National League of Cities, and finally, the National Ready Mixed Concrete Association; the National Stone, Sand, and Gravel Association; the Owner-Operator Independent Drivers Association;

the Portland Cement Association; and the Retail Industry Leaders Association.

The list I read is a partial list. The list that I read, frankly, is mostly Republican-leaning organizations.

Why have we not done our job? Why don't we already have a long-term transportation bill before us before the fund goes bust in 51 days? Why?

It is Congress's responsibility to act quickly to address our Nation's infrastructure needs. Every day that the Republicans fail to move forward with a bill, they are putting people at risk. This isn't about philosophy. This is about bread and butter. This is about getting to work safely. This is about driving with your family and not being fearful that the bridge you are on is going to fail.

I am always asked: Well, Senator, that is all well and good, but how are you going to pay for this?

Well, I have a lot of ideas, and I will lay them out. There are many ways to pay, and I will give just a sampling of ideas, and I will embrace these ideas. I will work with any Democrat or Republican on any one of these ideas.

Replace existing gas and diesel fuel fees with a user fee charged at the refinery based on the fuel price. In other words, do away with the gas tax and replace it with a refinery-based fuel fee. They did that in Virginia, and I think it is working well.

Increase existing gas and diesel fuel fees by indexing those fees to inflation, along with a refundable tax credit for low- and middle-income families to offset those costs. So we can have a modest increase of 6 cents, 7 cents, 8 cents on the gas tax and make it refundable to families earning $100,000 or less.

Assess a user fee on the sale of new and used vehicles. That is another idea.

Use revenue generated from repatriation of corporate earnings currently held overseas. That is international tax reform. We have a lot of money sitting abroad from corporations that have parked it there. They don't like the rate of their taxes. If you lower their tax, that money can come home, and we can use the taxes we collect to fund the highway trust fund. I have a bill on that with Senator PAUL. It is bipartisan. Join us. Join us and let's fix the problem.

How about this: Borrow money from the general fund, to be paid back from the stimulative effect of transportation infrastructure investments on the economy. When we make these investments, they generate so much employment and so much business that people will pay income taxes because they are working. These are millions of jobs, thousands of businesses.

Another way to pay for it: Apply a new, honor-based user fee on the number of miles each individual drives each year. So when you fill out a form to get your car registered, just tell me how many miles you traveled last year, there will be a modest fee, and we can help the trust fund.

By the way, I notice my friends want to use savings from reducing the overseas contingency operations account. They want to use that money. They used it for the military; why not use it for saving the trust fund? And how about the savings of uncollected revenues owed to the Federal Government? If we just collected one-third of those, we would meet the shortfall.

So, as I count these ideas, there are eight ideas that I have, and I am sure everybody has their own ideas. There is not a shortage of ideas. There is a bit of shortage of courage to come out and say the obvious. If your roof is about to collapse on your home, it will cost you something to fix it. Admit it upfront. No one is going to do it for free. No one is going to fix these 60,000-plus bridges for free. No one is going to build new highways for free. No one is going to build new transit systems for free. Grow up and pay for it. This is ridiculous.

I am speaking for myself. I will support any of these eight ideas or any combination of them. We know our country is in danger. Our people are in danger every day because of these structurally deficient bridges. If we don't do anything about it, we will be liable—maybe not in a court of law, but in my mind it is a moral responsibility. So I can support any of these ideas. Some of them are conservative ideas, and some of them are liberal ideas. I don't care. I want to pay for the highway trust fund.

The bottom line is that the only solution is a consensus-based, bipartisan 6-year transportation bill that will provide States and local communities with the funding and the certainty they need to build these multiyear projects and modernize our infrastructure.

This isn't rocket science. Choose one of the options. Add one of your own. Do a combination of these options. Let's have the courage and the moral fortitude to do what is our responsibility. We know our Nation's infrastructure is deteriorating. We are responsible for it. This is one Nation under God, and we have to act to protect our people. It is our job.

I think the clearest message was from President Eisenhower on this front, and President Reagan, who stepped up to the plate. President Reagan signed into law an increase in the gas tax. He was so proud. He said: I am proud to do this. We have to do this. Let me read his quote. He signed the surface transportation bill, which did increase the gas tax, and he said:

> Because of the prompt and bipartisan action of Congress, we can now ensure for our children a special part of their heritage—a network of highways and mass transit that has enabled our commerce to thrive, our country to grow, and our people to roam freely and easily to every corner of our land.

President Ronald Reagan. I was elected the same year he said this. I mean, I am giving away my age, but I was proud that my President understood this. I didn't agree with Ronald Reagan on a bunch of things. He said once: ''If you have seen one tree, you have seen them all.'' I never agreed with that.

But setting all of that aside, I agree with what he said. This is magnificent. Listen to this:

> Because of the prompt and bipartisan action of Congress, we can now ensure for our children a special part of their heritage—a network of highways and mass transit that has enabled our commerce to thrive, our country to grow, and our people to roam freely and easily to every corner of our land.

Another person whom I really admire on this subject is Senator INHOFE, my friend from Oklahoma, my chairman. I was his chairman for a few years—I think 8—and unfortunately for me I am no longer chairman, I am the ranking member. But I will tell you why we will do hand-to-hand combat on the environment—and we did that today. When it comes to infrastructure, we are very close. Do you know what he said? ''The conservative thing is to pass a bill instead of having the extensions.''

Anthony Foxx, our Transportation Secretary, and 11 of his predecessors offered an open letter to Congress expressing their support for passage of a long-term bill. Remember, this was signed by people who worked for—follow me—President Johnson, President Ford, President Reagan, President George Herbert Walker Bush, President Clinton, President George W. Bush, and President Obama. They offered an open letter and said this about the current situation:

> Never in our nation's history has America's transportation system been on a more unsustainable course. . . . So, what America needs is to break this cycle of governing crisis-to-crisis, only to enact a stopgap measure at the last moment. We need to make a commitment to the American people and the American economy.

That is four Republican Presidents and three Democratic Presidents—people from those administrations. My goodness, there is bipartisanship everywhere but here in this room.

I read the list of everybody who wants this bill, and it is very impressive: labor, business—small business, large business. It is extraordinary.

A survey by the National Association of Manufacturers of its members—one of our more conservative organizations—found that 65 percent don't believe our infrastructure is sufficient. We know from the Texas Institute study that traffic congestion in 2011 was $121 billion. We are wasting so much time in traffic. The cost to truck goods moving on our highway system—$27 billion in wasted time and diesel fuel.

So I hear a lot of talk about passing a long-term bill. I am pleased I am hearing that talk. I say to my colleagues, I hadn't heard of that, and now I am starting to hear my Republican friends say maybe we can do it. I think we need to do it. We still have 1.4 million fewer construction jobs than we had before the recession.

The clock is ticking. Failure is not an option. Let's get going. Let's come together and do the right thing. Pass the highway bill.

Thank you.

Mr. COONS. Mr. President, are we in a quorum call?

The PRESIDING OFFICER. The Senate is not in a quorum call.

EXPORT-IMPORT BANK

Mr. COONS. Mr. President, I have come to the floor today following on the speech just delivered by Senator BOXER, who highlighted her concern about a manufactured crisis—the impending expiration of the highway bill, which must be reauthorized by July 31. I come to speak to another manufactured crisis. We have to reauthorize the Export-Import Bank by June 30 or face the loss of its support for vital jobs in our economy that will happen with its expiration.

I am a big advocate for manufacturing here in the Senate and in my home State of Delaware, but I am not a big fan of manufactured crises. Both of these are unneeded, self-inflicted wounds that will create further drag on our economic recovery. I think we can and should find ways to work together across the aisle to reauthorize the Export-Import Bank.

For more than 80 years, the Export-Import Bank, commonly known as Ex-Im, has served as a vital tool to help American companies sell their goods around the world. By making loan guarantees and providing risk insurance and other financial products to American firms at market prices, the Bank has helped to ensure that American companies and their workers can compete anywhere in the world and at no cost to the American taxpayer. I will say that again: at no cost to the American taxpayer.

The Bank not only pays for itself, but it actually often runs a surplus. Last year alone, it returned $700 million to the U.S. Treasury. Today, the Ex-Im Bank helps American businesses sell nearly $30 billion in goods every single year and supports more than 150,000 American jobs.

The Bank is a government agency, however, and even though it costs taxpayers nothing and has an undeniably positive impact on our economy and on job creation, it remains unclear if this Congress will be able to come together to reauthorize it by June 30 and keep it running.

Unfortunately, some of my colleagues would like to close the Bank, and they are using arguments I think are unfounded and misguided to do so.

First, I have heard the Ex-Im Bank is somehow a government giveaway to large politically connected corporations. But the truth is the Bank helps companies of many different sizes, large and small.

In my home State of Delaware, for instance, the Ex-Im Bank has helped a company I know well—Voigt and Schweitzer, a hot-dip zinc galvanizing company. It has helped them to sell their products abroad. Voigt & Schweitzer has a few facilities around the United States, in addition to the one in New Castle, DE. At its Delaware location it provides galvanizing services for a range of steel products for export. V&S isn't a huge corporation. It has just a few dozen employees in Delaware. It is because of Ex-Im's support that it has been able to compete with other companies around the globe.

In fact, Ex-Im's support helped the firm's Delaware location earn the business to galvanize literally hundreds of bridges that were manufactured in Pennsylvania and being exported and sold to Africa—business that would have likely gone to competitors overseas without Ex-Im's help.

Now, Ex-Im does also help large corporations export their goods to countries around the world, but that support also benefits small and medium-sized businesses. For example, Boeing often receives significant support from the Ex-Im Bank, which helps it compete with international airplane manufacturers such as Airbus. I have heard Senators criticize this support, but the reality is it isn't just Boeing that benefits. This is an important point about how modern manufacturing and the integration of the supply chain work.

When Boeing manufactures a finished airplane, it doesn't make all of the plane's parts with its own factories and its own workforce. It, in fact, buys the vast majority of the component parts from much smaller manufacturers spread throughout the United States. From the brakes on the landing gear to the in-flight entertainment system, other companies make those parts and sell them to Boeing for the finished product. So when Ex-Im helps Boeing export a 747, it helps sustain tens of thousands of jobs for American workers at other smaller companies.

I have seen this myself in Delaware. Although Boeing directly employs in Delaware just 16 people, the company supports 1,300 jobs with 52 different Delaware companies. Let me give one example. A smallish company, Polymer Technologies, manufactures and sells thermal and acoustic insulation to Boeing for inclusion in their planes, which are then exported through the help of Ex-Im.

So when Ex-Im's opponents in this Chamber argue that this is all about a few big companies, that just isn't true. It also is vital to sustaining and supporting smaller manufacturers that are vital to our communities.

The next misplaced argument I have heard is that government shouldn't be supporting private companies, period. They should not be, as it were, picking winners and losers. But even to a supporter of the free market, the point of government is to step in where the private market fails to do so, and that is exactly what Ex-Im does.

When the Bank makes a loan to a business, it isn't replacing capital that would otherwise have come from a private bank. It supplements private capital or makes a private bank more inclined to put at risk its own capital through provision of political risk insurance. Much of the time Ex-Im serves as a lender of last resort and provides a loan where a private bank can't or won't.

So the Export-Import Bank isn't doing something the private sector should be doing. It is picking up where the market leaves off, and in doing so it helps to level the global playing field on which American companies compete.

The reality is that every single one of our trading partners provides the same type of support for their exports as the Ex-Im Bank does for ours. So they are picking winners. They are picking American winners on the global playing field.

For example, as Ex-Im's chairman, Fred Hochberg, has written, ''Ex-Im has given $590 billion in loans, guarantees, and insurance over its entire history but Chinese institutions''—Chinese export-financing institutions—''have provided an estimated $670 billion in just the past 2 years.''

In other words, China has done more in just 2 years to support the financing of their exporters than our Export-Import Bank has done in its entire 80-year history and at no cost to the taxpayer.

The bottom line is that American jobs are at stake in this debate, and if we fail to keep the doors open to the Export-Import Bank, we will fail a lot of American workers. Every year, Ex-Im supports hundreds of thousands of jobs, and shuttering it will put them at risk.

In fact, as the Wall Street Journal reported just this morning, American companies worry that global competition is ''so cutthroat,'' that they would ''be forced to move manufacturing overseas'' and to ship American manufacturing jobs out of the United States ''if the Ex-Im Bank isn't open.''

At a time when our economy is continuing to gain steam and Americans are going back to work—at a clip of 280,000 new jobs announced just last month—we need to continue to help American companies compete in markets around the world. The Ex-Im Bank is central to our competitiveness and our continued strength at home and abroad. It is critical that we act together to reauthorize it before the end of June. So I urge my colleagues to join this effort to help support American jobs, American manufacturing, and the American middle class.

Mr. President, for more than 20 years, the State Partnership Program—or SPP—has helped the United States to build closer sustained relationships with militaries and nations around the world. Although I will not call it up and make it pending at this moment, I want to take a few minutes to speak on the floor today about my amendment No. 1474 to the NDAA, an amendment that would significantly strengthen the State Partnership Program.

First established after the fall of the Soviet Union, the State Partnership Program was created to help countries transition their militaries from the Soviet model and enshrine the idea of civilian control of the military through professional and personal exchanges with our State National Guard units.

The SPP facilitates cooperation across all aspects of civil military affairs and, besides military relationships, encourages people-to-people ties at the State level. I have personally seen the benefits of this program through the participation of my home State National Guard in their State partnership with Trinidad and Tobago and the civilian control that it reinforces.

I have also seen it in farflung parts of the globe, from Liberia to Senegal to Tunisia on the African continent, where three different State Partnership Programs are actively at work providing training and support and resources for the military of those three nations.

The California National Guard, for example, currently has units that are helping Ukraine to push back against Russian aggression in eastern Ukraine, leveraging a deep and trusting relationship first established back in 1993.

Since its creation, the SPP has grown substantially. Today, it consists of 68 partnerships between U.S. National Guard units and foreign countries, with the 69th, between Kentucky's National Guard and the African nation of Djibouti, having just been signed. Djibouti is a nation that is actually the site of our only substantial military presence on the continent of Africa, and that State Partnership Program will help to strengthen, sustain, and reinforce our ongoing and vital security partnership with Djibouti, a nation that is sandwiched between Somalia and Yemen, countries currently in chaos and facing significant threats from Islamic terrorism.

That is just one example of how the State Partnership Program helps leverage the resources of our National Guard.

Traditionally, the program has needed to be reauthorized every 2 years, so I am happy this year that both the House and Senate have recognized its value and have decided to work together to permanently reauthorize it in their respective National Defense Authorization Act. However, there are a few changes we can make that would add to making the SPP more transparent, more efficient, and more effective, and that is what my amendment would do.

First, it would allow the Secretary of Defense to consolidate the various funding streams for the SPP, which right now come from over a half dozen different accounts scattered across DOD, which makes it more difficult to provide meaningful congressional sight. This amendment would allow the Defense Secretary to combine these funding sources into one National Guard fund to pay for personnel, training, operations, and equipment.

Second, my amendment would allow the National Guard to determine its core competencies and to help combatant commanders determine how best to leverage the National Guard to serve the needs of a partner country.

Last, my amendment would establish clear and enhanced reporting requirements so we can better track the annual performance of our units and make modifications where needed to enhance the program's effectiveness.

Critically, this amendment would not increase the program's costs at all. This amendment, which is based on the State Partnership Program Enhancement Act and currently has 9 Republican and 12 Democratic Senators, including myself, Senator LINDSEY GRAHAM of South Carolina, Senator PAT LEAHY of Vermont, and Senator JONI ERNST of Iowa, enjoys broad bipartisan support from a wide range of States whose National Guards have participated and benefited from the State Partnership Program.

The amendment is enthusiastically supported by the National Guard Association of the United States, the National Guard Bureau, and the Adjutants General. It would take important steps to strengthening a program that is essential to many of our international partnerships, and I urge my colleagues to support it.

With that, I thank the Chair, and I yield the floor.

Mr. WARNER. Mr. President, I join my Virginia colleague Senator TIM KAINE in expressing concern over the chairman's measure to cut $1.7 billion in funding from specific operations and maintenance accounts in an effort to streamline defense headquarters functions.

The Department of Defense is in the midst of implementing a 20 percent headquarters reduction that defense officials have planned over time to ensure that consequences of the reductions are known and managed. Like my colleague, I am concerned that the chairman's proposed legislation would require additional headquarters reductions, the results of which have not been properly considered.

While I support continued efficiency gains within the Department of Defense, including—where merited—reducing headquarters functions, I believe that before such cuts are taken, the Department must conduct a thorough analysis of the best methods to streamline their organizations for the most efficient staffing solutions while remaining viable and effective.

At a time when department officials are managing through enormous budget pressure in an increasingly complex national security environment, I fear the Department will be forced to reduce funding to critical programs.

Finally, the men and women who will likely bear the brunt of these cuts are performing the very work that Congress charged the Department of Defense to conduct. Even this authorization includes additional reports, studies, and demands for improvement in areas like program management, personnel planning, acquisition, and sexual assault. These programs require a professional cadre to conduct the required analysis and propose recommendations for improvement.

I look forward to passing a defense authorization that adequately supports the Department that has been at war for nearly 15 years.

Mr. KAINE. Mr. President, I am pleased the Senate is debating the National Defense Authorization Act for fiscal year 2016. Senators MCCAIN and REED, with help from my colleagues and me on the Senate Armed Services Committee, have worked tirelessly throughout the spring on these important military issues. Our committee prides itself on taking a bipartisan and measured approach to reforming and providing oversight to the Department of Defense. I believe we largely succeeded in this endeavor, but I remain gravely concerned about the chairman's proposals to streamline Department of Defense Headquarters by cutting funding to specific operations and maintenance, O&M, accounts.

The Department of Defense already implemented a 20 percent reduction of headquarters, which began this year and continues through 2019. Planning for the reduction began several years ago, affording the Department adequate time to ensure compliance with various directives, including requirements of the Goldwater-Nichols Act that established the division in roles among the service chiefs and combatant commanders. I am concerned the chairman's proposed legislation this year, requiring additional headquarters reductions, will force the Department of Defense to find efficiencies that will blur the lines between service and warfighting functions, undermining the bedrock reforms established by Goldwater-Nichols.

I support reducing the magnitude of these cuts, while allowing the Department to conduct a thorough analysis of the best methods to streamline organizations for the most efficient staffing solutions while remaining viable and effective.

The chairman's specific proposed reductions are not supported by any report or study. Instead, they are based on a perception of unnecessary growth based on anecdotal evidence and nebulous data-sets fueled a $1.7 billion cut to several operations and maintenance accounts.

To the chairman's point, there has undoubtedly been a growth in headquarters over the past decade. Areas that saw significant increases include cyber warfare and special operations. USCYBERCOM did not exist a decade ago, but now has almost 6,000 employees. Special Operations Command is forecasted to swell to over 70,000 by 2017, but both headquarters are excluded from consideration for reduction, against the requests of the DOD

to leave everything on the table if forced to act on this provision.

The timing and magnitude of these cuts are so severe that I fear the Department will be forced to reduce funding to critical programs associated with the targeted accounts. Some key programs associated with these accounts include military burial honors, suicide prevention, radioactive waste disposal, nuclear command and control networks, acquisition support, veteran hiring programs, and installation fire departments. Many of these programs are tied to our Nation's commitment to our servicemembers and veterans and should not be subjected to such drastic cuts without due consideration of the downstream effects.

Finally, the men and women who will likely bear the brunt of these cuts are performing the very work that Congress charged the Department of Defense to conduct. Even this authorization includes additional reports, studies, and demands for improvement in areas like program management, acquisition, and sexual assault. These programs require a professional cadre to conduct the required analysis and propose recommendations for improvement. Asking our workforce to bear additional oversight and program management functions while cutting their funding is illogical and wrong.

The PRESIDING OFFICER. The Senator from Oregon.

CYBERSECURITY INFORMATION SHARING ACT

Mr. WYDEN. Mr. President, I wish to speak this afternoon about a controversial proposal, the Cybersecurity Information Sharing Act, otherwise known as CISA, which was filed yesterday as an amendment to the Defense authorization bill.

I want to begin by saying to the Senate that I believe tacking this legislation onto the Defense bill would, in my view, be a significant mistake. I expect our colleagues are going to have a wide range of views about this legislation, and I hope the Senate can agree that bills as controversial as this one ought to be subject to public debate and an open-ended process, not stapled onto unrelated legislation with only a modest amount of discussion.

This is particularly true given the issue of cyber security, which is going to have a significant impact on the security and the well-being of the American people and obviously the consumer rights and the privacy of law-abiding Americans. Because it is designed to increase government collection of information from private companies, I am of the view that for the Senate to have this expansion of collecting so much information about the people of the United States, for it to have real legitimacy in the eyes of the public, it is important to have open debate, with votes on amendments from Senators who have a wide variety of opinions on the issue of cyber security. Trying to rush this bill through the Senate, in my view, is not going to increase public confidence.

So let me be clear about the process and talk a bit about the substance of the legislation as well. I believe tacking it onto the Defense bill is a flawed process. But I think there are also significant flaws with the substance of the legislation as well. Dozens of independent experts agree this legislation will have serious consequences and do little to make our Nation more secure at a time when cyber threats are very real. The issue of cyber threats requires more than a placebo, and this legislation is a bandaid on a gaping wound. I believe the Senate, having the time for adequate reflection and amendment, can do better.

In beginning, I would like the Senate to know just how much controversy and concern this legislation has generated among those who are considered independent experts on cyber security. Shortly before the Intelligence Committee, which I have been honored to serve on for more than 14 years—shortly before the committee marked up this legislation, a coalition of nearly 50 organizations and security experts wrote to the members of the Intelligence Committee expressing serious concerns about the legislation.

Mr. President, I ask unanimous consent that this letter be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

Re Cyber Threat Information Sharing Bills

APRIL 16, 2015.

Senator DIANNE FEINSTEIN,
Hart Senate Office Building, Washington, DC.
Congressman ADAM SCHIFF,
Rayburn House Office Building, Washington, DC.
Congressman MICHAEL MCCAUL,
Cannon House Office Building, Washington, DC.
Senator RICHARD BURR,
Russell Senate Office Building, Washington, DC.
Congressman DEVIN NUNES,
Longworth House Office Building, Washington, DC.

DEAR SENATOR BURR, SENATOR FEINSTEIN, AND REPRESENTATIVES NUNES, SCHIFF, AND MCCAUL: We are writing you today as technologists, academics, and computer and network security professionals who research, report on, and defend against Internet security threats. Among us are antivirus and threat signature developers, security researchers and analysts, and system administrators charged with securing networks. We have devoted our careers to building security technologies, and to protecting networks, computers, and critical infrastructure against a wide variety of even highly sophisticated attacks.

We do not need new legal authorities to share information that helps us protect our systems from future attacks. When a system is attacked, the compromise will leave a trail, and investigators can collect these bread crumbs. Some of that data empowers other system operators to check and see if they, too, have been attacked, and also to guard against being similarly attacked in the future. Generally speaking, security practitioners can and do share this information with each other and with the federal government while still complying with our obligations under federal privacy law.

Significantly, threat data that security professionals use to protect networks from future attacks is a far more narrow category of information than those included in the bills being considered by Congress, and will only rarely contain private information. In those rare cases, we generally scrub the data without losing the effectiveness of the threat signature.

These are some common categories of data that we share to figure out if systems have been compromised (indicators of compromise, or IoCs) and to mitigate future threats:

Malware file names, code, and hashes

Objects (code) that communicate with malware

Compile times: data about the conversion of source code to binary code

File size

File path location: where on the computer system malware files are stored

Registry keys: configuration settings for low-level operating system and applications

Memory process or running service information

Attached to this letter is an actual example of a threat signature containing data that helps system administrators secure their networks. You'll see that the information does not contain users' private information.

Waiving privacy rights will not make security sharing better. The more narrowly security practitioners can define these IoCs and the less personal information that is in them, the better. Private information about individual users is often a detriment in developing threat signatures because we need to be able to identify an attack no matter where it comes from and no matter who the target is. Any bill that allows for and results in significant sharing of personal information could decrease the signal-to-noise ratio and make IoCs less actionable.

Further, sharing users' private information creates new security risks. Here are just three examples: First, any IoC that contains personal information exacerbates the danger of false-positives, that innocent behavior will erroneously be classified as a threat. Second, distribution of private data like passwords could expose our users to unauthorized access, since, unfortunately, many people use the same password across multiple sites. Third, private data contained in personal emails or other messages can be abused by criminals developing targeted phishing attacks in which they masquerade as known and trusted correspondents.

For these reasons, we do not support any of the three information sharing bills currently under consideration—the Cybersecurity Information Sharing Act (CISA), the Protecting Cyber Networks Act (PCNA), or the National Cybersecurity Protection Advancement Act of 2015. These bills permit overbroad sharing far beyond the IoCs described above that are necessary to respond to an attack, including all ''harms'' of an attack. This excess sharing will not aid cybersecurity, but would significantly harm privacy and could actually undermine our ability to effectively respond to threats.

As a general rule, when we do need to share addressing information, we are sharing the addresses of servers which are used to host malware, or to which a compromised computer will connect for the exfiltration of data. In these cases, this addressing information helps potential victims block malicious incoming connections. These addresses do not belong to subscribers or customers of the victims of a security breach or of our clients whose systems we are helping to secure. Sharing this kind of addressing is a common current practice. We do not see the need for new authorities to enable this sharing.

Before any information sharing bill moves further, it should be improved to contain at least the following three features:

1. Narrowly define the categories of information to be shared as only those needed for securing systems against future attacks;

2. Require firms to effectively scrub all personally identifying information and other private data not necessary to identify or respond to a threat; and

3. Not allow the shared information to be used for anything other than securing systems.

We appreciate your interest in making our networks more secure, but the legislation proposed does not materially further that goal, and at the same time it puts our users' privacy at risk. These bills weaken privacy law without promoting security. We urge you to reject them.

Sincerely,

Ben Adida; Jacob Appelbaum, Security and privacy researcher, The Tor Project; Sergey Bratus, Research Associate Professor, Computer Science Department, Dartmouth College; Eric Brunner-Williams, CTO, Wampumpeag; Dominique Brezinski, Principal Security Engineer, Amazon.com; Jon Callas; Katherine Carpenter, Independent Consultant; Antonios A. Chariton, Security Researcher, Institute of Computer Science, Foundation of Research and Technology—Hellas; Stephen Checkoway, Assistant Research Professor, Johns Hopkins University; Gordon Cook, Technologist, writer, editor and publisher of ''COOK report on Internet Protocol'' since 1992; Shaun Cooley, Distinguished Engineer, Cisco; John Covici, Systems Administrator, Covici Computer Systems; Tom Cross, CTO, Drawbridge Networks; David L. Dill, Professor of Computer Science, Stanford University; A. Riley Eller, Chief Technology Officer, CoCo Communications Corp; Rik Farrow, USENIX.

Robert G. Ferrell, Special Agent (retired), U.S. Dept of Defense; Kevin Finisterre, Owner, DigitalMunition; Bryan Ford, Associate Professor of Computer Science, Yale University; Dr. Richard Forno, Affiliate, Stanford Center for Internet and Society; Paul Ferguson, Vice President, Threat Intelligence; Jim Fruchterman, Benetech; Kevin Gennuso, Information Security Professional; Dan Gillmor. Teacher and technology writer; Sharon Goldberg, assistant professor, Computer Science Department, Boston University; Joe Grand, Principal Engineer, Grand Idea Studio, Inc.; Thaddeus T Grugq, independent security researcher; J. Alex Halderman, Morris Wellman Faculty Development Assistant Professor of Computer Science and Engineering, University of Michigan, Director, University of Michigan Center for Computer Security and Society; Professor Carl Hewitt, Emeritus EECS MIT; Gary Knott, PhD (Stanford CS, 1975), CEO, Civilized Software; Rich Kulawiec, Senior Internet Security Architect, Fire on the Mountain, LLC; Ryan Lackey; Product, CloudFlare, Inc.

Ronald L. Larsen, Dean and Professor, School of Information Sciences, University of Pittsburgh; Christopher Liljenstolpe, Chief architect for AS3561 (at the time about 30% of the Internet backbone by traffic) and AS1221 (Australia's main Internet infrastructure); Ralph Logan, Partner, Logan Haile, LP; Robert J. Lupo, Senior Security Engineer ''sales team'', IBM inc.; Marc Maiffret, Former CTO BeyondTrust; Steve Manzuik, Director of Security Research, Duo Security; Ryan Maple. Information security professional; Brian Martin, President Open Security Foundation (OSF); Morgan Marquis-Boire; Aaron Massey, Postdoctoral Fellow, School of Interactive Computing, Georgia Institute of Technology; Andrew McConachie. Network engineer with experience working on Internet infrastructure; Daniel L. McDonald, RTI Advocate and Security Point-of-Contact, illumos Project; Alexander McMillen, Mission critical datacenter and cloud services expert; Charlie Miller, Security Engineer at Twitter; HD Moore, Chief Research Officer, Rapid7.

Joseph ''Jay'' Moran, Vice President of Cimpress Technology Operations; Peter G. Neumann, Senior Principal Scientist, SRI International Moderator of the ACM Risks Forum (risks.org); Jesus Oquendo, Information Security Researcher, E-Fensive Security Strategies; Ken Pfeil, CISO, Pioneer investments; Benjamin C. Pierce, Professor of Computer and Information Science, University of Pennsylvania; Ryan Rawdon, Network and Security Engineer; Bruce Schneier, security researcher and cryptographer, published seminal works on applied cryptography; Sid Stamm, Ph.D., Principal Engineer, Security and Privacy, Mozilla; Visiting Assistant Professor of Computer Science, Rose-Hulman Institute of Technology; Armando Stettner, Technology Consultant; Matt Suiche, Staff Engineer, VMware.

C. Thomas (Space Rogue), Security Strategist Tenable Network Security; Arrigo Triulzi, independent security consultant; Doug Turner, Sr. Director—Privacy, Security, Networking, Mozilla Corporation; Daniel Paul Veditz, Principal Security Engineer, Mozilla, Co-chair Web Application Security Working Group, W3C; David Wagner, Professor of Computer Science, University of California, Berkeley; Dan S. Wallach, Professor, Department of Computer Science and Rice Scholar, Baker Institute for Public Policy, Rice University; Jonathan Weinberg, Professor of Law, Wayne State University; Stephen Wilson, Managing Director and Founder, Lockstep Technologies; Chris Wysopal, CTO and co-founder Veracode, Inc.; Stefano Zanero, Board of Governors member, IEEE Computer Society.

Mr. WYDEN. The signers of the letter expressed very serious concerns about the legislation and were particularly concerned it would ''significantly undermine privacy and civil liberties.'' Unfortunately, as the signers of the legislation will report, these concerns were not adequately addressed in the committee markup.

Shortly after the committee markup, a group of 65 technologists and cyber security professionals wrote to Chairman BURR and Vice Chairman FEINSTEIN expressing their opposition to this legislation.

Mr. President, I ask unanimous consent that this letter be printed in the RECORD as well.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

MARCH 2, 2015.

Chairman RICHARD BURR,
Senate Select Committee on Intelligence, U.S. Senate.

Vice Chairman, DIANNE FEINSTEIN,
Senate Select Committee on Intelligence, U.S. Senate.

DEAR CHAIRMAN BURR, VICE CHAIRMAN FEINSTEIN, AND MEMBERS OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE: We the undersigned civil society organizations, security experts, and academics write to explain how the Cybersecurity Information Sharing Act of 2015 (CISA), would significantly undermine privacy and civil liberties. We now know that the National Security Agency (NSA) has secretly collected the personal information of millions of users, and the revelation of these programs has created a strong need to rein in, rather than expand, government surveillance. CISA disregards the fact that information sharing can—and to be truly effective, must—offer both security and robust privacy protections. The legislation fails to achieve these critical objectives by including:

Automatic NSA access to personal information shared with a governmental entity;

Inadequate protections prior to sharing;

Dangerous authorization for countermeasures; and

Overbroad authorization for law enforcement use.

For the following reasons, we urge rejection of CISA in its current form:

Automatic NSA Access to Personal Information and Communications: Since the summer of 2013, NSA surveillance activities, such as the telephony metadata bulk collection program and the PRISM program, have raised nationwide alarm. CISA ignores these objections, and requires real time dissemination to military and intelligence agencies, including the NSA. Congress should be working to limit the NSA's overbroad authorities to conduct surveillance, rather than passing a bill that would increase the NSA's access to personal information and private communications.

Automatic sharing with NSA risks not only privacy, but also effectiveness. During a recent House Intelligence Committee hearing, NSA Director Admiral Mike Rogers stated that sharing threat indicators without filtering out personal data would slow operations and negatively impact NSA's cyber defense activities. Further, in the wake of revelations regarding the PRISM program, major tech companies stated that they would not voluntarily share users' information with the NSA. Automated NSA access could thus disincentivize sharing, undercutting the key goal of the legislation.

Inadequate Protections Prior to Sharing: CISA does not effectively require private entities to strip out information that identifies a specific person prior to sharing cyber threat indicators with the government, a fundamental and important privacy protection. While the bill requires that companies ''review'' cyber threat indicators for information that identifies a specific person and sometimes remove it, the bill contains no standard to ensure that this review effort is—at a minimum—reasonable.

Further, the bill requires companies to remove that information only for individuals that it knows are ''not directly related to a cybersecurity threat.'' This could encourage companies to retain data by default, unnecessarily exposing the information of innocent bystanders and victims to the government, and making it available to law enforcement for a myriad of investigative uses. Legislation should instead require that prior to sharing, companies make at least a reasonable effort to identify all personally identifiable information and, unless it is necessary to counter the cyber threat before sharing any indicators with the government, remove it. The default should be to preserve privacy, rather than to sacrifice it.

Dangerous Authorization for Countermeasures: CISA authorizes countermeasures ''notwithstanding any law,'' including the federal Computer Fraud and Abuse Act. As amended by CISA, federal law would permit companies to retaliate against a perceived threat in a manner that may cause significant harm, and undermine cybersecurity. CISA provides that countermeasures must be ''operated on'' one's own information systems, but may have off-networks effects—including harmful effects to external systems—so long as the countermeasures do not ''intentionally'' destroy other entities' systems. Given the risks of misattribution and

escalation posed by offensive cyber activities—as well as the potential for misappropriation—this is highly inadvisable. CISA permits companies to recklessly deploy countermeasures that damage networks belonging to innocent bystanders, such as a hospital or emergency responders that attackers use as proxies to hide behind, so long as the deploying company does not intend that the countermeasure result in harm. CISA's authorization would not only inadvisably wipe away the Computer Fraud and Abuse Act's current prohibition against these activities, it would be dangerous to internet security.

Overbroad Law Enforcement Use: Law enforcement use of information shared for cybersecurity purposes should be limited to prosecuting specific cyber crimes identified in the bill and preventing imminent loss of life or serious bodily harm. CISA goes far beyond this, and permits law enforcement to use information it receives for investigations and prosecutions of a wide range of crimes involving any level of physical force, including those that involve no threat of death or significant bodily harm, as well as for terrorism investigations, which have served as the basis for overbroad collection programs, and any alleged violations of various provisions of the Espionage Act. The lack of use limitations creates yet another loophole for law enforcement to conduct backdoor searches on Americans—including searches of digital communications that would otherwise require law enforcement to obtain a warrant based on probable cause. This undermines Fourth Amendment protections and constitutional principles.

Cybersecurity legislation should be designed to increase digital hygiene and identify and remediate advanced threats, not create surveillance authorities that would compromise essential privacy rights, and undermine security. Accordingly, we urge that the Committee not approve this bill without addressing these concerns.

Thank you for your consideration,

Civil Society Organizations—Access; American-Arab Anti-Discrimination Committee; American Library Association; Advocacy for Principled Action in Government; American Civil Liberties Union; Association of Research Libraries; Bill of Rights Defense Committee; Brennan Center for Justice; Center for Democracy & Technology; Center for National Security Studies; Competitive Enterprise Institute; Constitutional Alliance; The Constitution Project; Council on American Islamic Relations; Cyber Policy Project; Defending Dissent Foundation; Demand Progress; Electronic Frontier Foundation Free Press Action Fund FreedomWorks; Liberty Coalition; National Association of Criminal Defense; Lawyers; New America's Open Technology Institute; Project on Government Oversight; R Street Institute; Sunlight Foundation.

Security Experts and Academics—Ben Adida, Cryptographer; Jacob Appelbaum, The Tor Project; Alvaro Bedoya, Center on Privacy and Technology at Georgetown Law; Brian Behlendorf; David J Farber, University of Pennsylvania; J. Alex Halderman, University of Michigan; Joan Feigenbaum, Yale University; Bryan Ford, Yale University; Matthew D. Green, Johns Hopkins University; Daniel Kahn Gillmor, Technologist; Susan Landau, Worcester Polytechnic Institute; Sascha Meinrath, X-Lab; Peter G, Neumann, SRI International; Ronald L. Rivest, Massachusetts Institute of Technology; Phillip Rogaway, University of California, Davis; Bruce Schneier, Cryptographer and Security Specialist; Christopher Soghoian, Technologist; Gene Spafford, Purdue University; Micah Sherr, Georgetown University; Adam Shostack; Dan S. Wallach, Rice University; Nicholas Weaver, University of California at Berkeley.

Mr. WYDEN. This is a particularly important letter. We have some of the most distinguished independent experts from across the country—whether Amazon or Sysco, Stanford University, Dartmouth, some of the leading experts in the private sector and academia—expressing real concerns about this legislation and its House companion.

From their letter:

We appreciate your interest in making our networks more secure, but the legislation proposed does not materially further that goal, and at the same time it puts our users' privacy at risk. These bills weaken privacy law without promoting security. We urge you to reject them.

The reason I want our colleagues to be aware that these distinguished scientists in Silicon Valley, and literally every corner of the country, are so concerned is that the American people want both security and liberty—and they understand the two are not mutually exclusive. What this distinguished group of experts has just said is this ''weaken[s] privacy law without promoting security.'' I hope the Senate will review what these experts are saying.

Along the same lines, I note that the Christian Science Monitor recently polled a group of more than 78 high-profile security and privacy experts from across government, think tanks, and the private sector. With these experts, they asked if legislation along the lines of this bill—this bill which has been attached to the Defense authorization. These experts were asked if this legislation would significantly reduce security breaches, and 87 percent said it would not. Many of them noted—a concern I have noted in opposing the legislation—that incentivizing private companies to share information about security threats is a very worthwhile proposition, a worthwhile thing to do. But they go on to say that bills like this are going to have limited value in that area and would have significant negative consequences.

Now, many of my colleagues may have some disagreement with some of the dozens and dozens of independent experts I have just mentioned. Some of them may agree with the 13 percent of those experts who said this bill will do a lot to reduce security breaches. That is their right, and that is what a good Senate debate would be all about. But what the Senate should not do is pretend that this legislation is uncontroversial and try to rush it through without substantial revisions and the chance for Senators on both sides of the aisle to be heard.

Now, I think we all understand why some in the Senate would feel we have to move immediately on this issue and in effect be tempted to rush to action here. We have all understood there have been a number of recent high-profile hacks that have drawn attention to the need to improve our Nation's cyber security—and I don't disagree with the importance of that at all.

For example, a major company in Oregon was hacked by the Chinese simply because they were trying to enforce their rights under trade law.

So this is not some abstract issue for the people I represent. We have seen it in my home State.

So these high-profile hacks, like the one we saw here recently, is obviously drawing attention to the need to improve cyber security. The recent compromise of a very large amount of Office of Personnel Management data is obviously the latest of these, but it is certainly not going to be the last.

Every single time I read about these kind of hacks, what I do is—and I have a very talented staff from the Intelligence Committee and my own office to assist me—I try to reach out and talk to experts in the field about ways to improve cyber security. But that doesn't mean every single piece of legislation with the word ''cyber security'' in it is automatically a good idea that ought to be blessed without revision in the Senate.

The fact is, this particular cyber security bill is largely focused on trying to make it more difficult for individuals to be able to take on corporations. I understand why the U.S. Chamber of Commerce likes it so much. They have always been concerned about the rights of the large corporations. Sometimes the inevitable is, well, we are concerned about the large corporations, let's make it harder for individuals to be able to get a fair shake in the marketplace. But in my judgment, the actual cyber security value of this bill would be very limited, and the consequences for those individuals who are trying to get a fair shake would be quite serious.

I am going to turn in a moment to the substance of the CISA bill to explain why I consider it so problematic and why it needs a major revision. But first I am going to take just a few minutes to discuss proposals that I believe would actually make a difference in terms of improving American cyber security.

First, the most effective way to improve cyber security is to ensure that network owners take responsibility for the security of their networks and effectively implement good security practices. This proposal was the centerpiece of a 2012 bill called the Lieberman-Collins cyber security bill, and in my view that legislation was just a few changes away from being good cyber security law. Unfortunately, the notion of having the government create even voluntary standards for private companies was strongly opposed by the U.S. Chamber of Commerce and the Congress has not revisited it since.

Beyond ensuring that network owners take responsibility and implement good security practices, it is also important to ensure that government agencies do not deliberately weaken security standards.

I know the Presiding Officer in the Senate has a great interest, as I do, in

innovation and American competitiveness. It is pretty hard—when we say the words: The American Government is actually thinking, as the FBI Director has talked about, about requiring companies to build weaknesses into their products—it is pretty hard to get your arms around this theory, not the least of which is the reason that once the good guys have the keys, the bad guys will also have the keys, which will facilitate cyber hacking.

I have been skeptical of these statements from senior FBI officials suggesting that U.S. hardware and software companies should be required, as I would characterize it, to weaken the security of their products because encryption and other advanced security measures are a key part, a key compound of actually improving cyber security.

I was pleased to see that in the other body, just last week, a new amendment from Representatives MASSIE and LOFGREN to prevent the government from deliberately weakening encryption standards was voted on, and I am very hopeful the Senate will eventually follow suit. In fact, I offered that concept in the Intelligence Committee, and regrettably it did not pass.

With regard to government-held data, it is absolutely imperative that Federal agencies receive the funding and expertise they need to develop and implement strong network security programs and to ensure that they have the technical and administrative controls in place to combat a wide range of cyber security threats.

I also believe our government needs to be in a stronger position to recruit and retain a capable Federal cyber security workforce by ensuring that cyber security professionals can find opportunities in government that are as rewarding as those in the private sector. In order to ensure that there are enough professionals to fill positions in both the private sector and the government, it is obvious that there is going to need to be an investment in the education of the next generation of cyber security leaders.

As we talk about responsible approaches to deal with these cyber issues, I would like to note that I consider the Consumer Privacy Protection Act—a piece of legislation initiated by Senator LEAHY—to be another step in the right direction. This legislation creates a comprehensive approach to data security by requiring companies to build a cyber security program that can defend against cyber attacks and prevent data breaches. It also protects a wide range of personal information, not just name or financial account information but also online user names and passwords, information about a person's geolocation, and access to private digital photographs and videos.

Unlike CISA, this legislation would, in my view, provide real tools to address the kinds of recent cyber attacks we have seen in the news, such as the celebrity photo hack. Unlike CISA, it would also empower individuals by requiring companies to notify consumers if their information has been lost and would protect the rights offered under some State laws for consumers to sue in the event of a privacy incident. The Consumer Privacy Protection Act is the right kind of responsible, thoughtful approach to cyber security, which is legislation that will help us get an added measure of security and public protection, while at the same time protecting the individual liberties and the privacy of our people.

Finally, in my judgment, our country needs to be willing to impose consequences on foreign entities that attempt to hack into American networks and steal large quantities of valuable data. These hacks are undermining our national security, our economic competitiveness, and the personal privacy of huge numbers of Americans. These consequences should draw on the full range of American power, depending on the nature of the hack and the entity responsible.

It would be a failure of American imagination to say that the only way to respond to foreign hacking is to have our military and intelligence agencies ''hack back,'' as the concept has been known, at the parties responsible. We are the most powerful country in the world, and our government has a wide variety of tools at its disposal, including economic sanctions, law enforcement, and multilateral diplomacy. And building a multifaceted strategy to deter foreign hacking is going to require all of those kinds of tools I have mentioned by way of articulating responsible steps to deal with cyber security, steps that protect both our security and liberty. All of those tools are ones we will have to draw on.

Having laid out ways that the Senate on a bipartisan basis can improve cyber security, I want to turn to the proposal in detail that is now in front of the Senate. As I have said, I believe it makes sense to encourage private companies to share information about cyber security threats. Cyber is a problem. Sharing information can be useful, but it is also vital that information sharing not be bereft of privacy protections for law-abiding Americans.

Cyber security is a problem. Information sharing is a plus. But let's make no mistake about it—an information-sharing bill that lacks privacy protections really is not a cyber security bill; it is a surveillance bill. That is what has been one of my major concerns about this legislation, that the legislation in front of the Senate—we talked about the flaws in the process, but substantively, if you have an information-sharing bill that lacks adequate privacy protections, it is a surveillance bill by another name.

When the Senate Intelligence Committee voted on the CISA bill, I opposed it. I opposed it because I believe its insufficient privacy protections will lead to large volumes of Americans' personal information, personal information from law-abiding Americans who have done nothing wrong—that they will be faced with the prospect that their information is shared with the government even when that information is not needed for cyber security. When I say ''personal information,'' I am talking about the contents of emails, financial information, and what amounts to any data at all that is stored electronically.

Some of my colleagues have stressed that companies will have a choice about whether to participate in this information-sharing part of the legislation. That is true, but while corporations will have a choice about whether to participate, they will be able to do so without the knowledge or consent of their customers, and they will receive broad liability protections when they do so. The CISA bill as written trumps all Federal privacy laws.

Furthermore, once this information is shared with the government, government agencies will be permitted to use it for a wide variety of purposes unrelated to cyber security. The bill creates what I consider to be a double standard—really a bizarre double standard in that private information that is shared about individuals can be used for a variety of non-cyber security purposes, including law enforcement action against these individuals, but information about the companies supplying that information generally may not be used to police those companies.

I will tell you, I think that will be pretty hard to explain at a townhall meeting in virtually any corner of America because I believe it is wrong to say that the privacy rights of corporations matter more than the privacy rights of individual Americans.

I expect that some colleagues will say that it is not their intent to authorize this excessively broad collection. The argument will be that this is legislation to encourage companies to share information about actual cyber security threats, such as lines of malicious code and signatures of hostile cyber actors. Again, I would say to colleagues that I am all for encouraging companies to share information about genuine security threats, but if you read the language that is now before the Senate in the cyber security bill, the language of that bill is much broader than just sharing information about genuine security threats.

If Senators want to pass a bill that is focused on real cyber security threats and includes real protection for Americans' privacy, then the Senate should add language specifying that companies should only provide the government with individuals' personal information if it is necessary to describe a cyber security threat. That does not seem to me to be an unreasonable protection for the privacy of Americans, that the Senate would adopt language specifying that the companies provide the government with individuals' personal information if it is necessary to

describe a cyber threat. That is pretty obvious.

We can explain that, I would say to the distinguished President of the Senate, at a townhall meeting, that if it is related to a cyber security threat, then the companies would provide individuals' personal information. But this would discourage companies from unnecessarily sharing large amounts of their customers' private information with the government.

Unfortunately, the cyber security bill in front of the Senate now takes the opposite approach. It only requires companies to withhold information that is known at the time of sharing to be personal information unrelated to cyber security. This approach will clearly discourage companies from closely reviewing the information that they share and will lead to a much greater amount of Americans' personal information being transferred needlessly to government agencies.

I hope that here in the Senate there will be an opportunity to carefully consider the potential consequences of this legislation before voting to rush it through by an expedited process.

I have said here several times that cyber security is a real problem, and policymakers are going to have to deal with it. In fact, I will go so far as to say that the issue of cyber security is going to be an ongoing and enduring challenge of the digital age. It is my view that every Senator who serves in this body today can expect to deal with cyber security questions for the rest of their career in public service. Voting to rush a bill through, however, is not going to make these problems somehow go away, and it will have real consequences for our constituents for years to come, and in particular, it will not make us safer and will jeopardize the rights of individual Americans.

Before I wrap up, I believe it is important and I have an obligation to draw my colleagues' attention to one final issue. As of this afternoon, there is a secret Justice Department legal opinion that is of clear relevance to this debate that continues to be withheld from the public. This opinion remains classified. The Senate rules prohibit me from describing it in detail. But I can say that it interprets common commercial service agreements and that in my judgment is inconsistent with the public's understanding of the law.

So this gets back to a question I have talked about on the floor often, which is secret law, when the public reads one thing and there is a secret interpretation that goes in another direction and it contributes to the public's cynicism about Washington.

As always, I certainly see it as my job to say that colleagues can decide whether to take my counsel, but I believe any Senator who votes for this legislation, without reading this secret Justice Department legal opinion I have referred to, is voting without a full understanding of the relevant legal landscape. If Senators do not understand how these common commercial service agreements have been interpreted by the executive branch, then it will be harder for the Senate to have a fully informed debate on the cyber security legislation, whether it is considered now or later.

I would also like to note for the record that I have repeatedly asked the Justice Department to withdraw this opinion and to make it public so anyone who is party to one of these commercial service agreements can decide whether their agreement ought to be revised. The Justice Department has chosen not to take my advice on either of my suggestions.

In public testimony before the Senate Intelligence Committee, the deputy head of the Justice Department's Office of Legal Counsel told me she personally would not rely on this opinion today, and I appreciate her view on that matter. Yet, until the opinion is withdrawn, I believe Senators should be concerned about other government officials choosing to rely on it at any time. In my judgment, that is a very clear instance of the government developing what is essentially secret law—law that is at variance with what you read if you are in a coffee shop in Arkansas or Utah or anywhere else.

The reality is, as I have said often on the floor, operations always have to be secret, as do the sources and methods. Chairman HATCH remembers this from his service on the Intelligence Committee. Operations always have to be secret, but the law ought to be public because that is how the American people have confidence in how we make decisions in our Republic.

I will close by saying it is quite obvious at this point that I have significant reservations about the cyber security bill. I believe a number of Senators are going to share these concerns. I will let them speak for themselves, although I believe Senator LEAHY's strong statement yesterday was certainly on point. Yet I will also say, even to my colleagues who are inclined to vote for this bill, that I hope all Senators will think about whether this is an appropriate process for this sort of legislation.

I have already said I believe Senators are going to be dealing with cyber security questions for the rest of their time in public service, because in the digital age, I think we are going to see a constant evolution in this field with respect to these threats and both the technical and political concerns that are raised by them.

Should the Senate be rushing a bill like this through by tacking it onto an unrelated defense measure? Is this the best way to show the American people, once again, that security and liberty are not mutually exclusive and that it is possible to do both?

If Senators share the concerns I have raised, I hope they will oppose the cyber security amendment if it is brought up for a vote on the Defense bill. I hope Senators will support this issue, which has been brought to the floor under a different process—a process that involves regular order, so every Senator on both sides of the aisle will have an opportunity to make the revisions I believe it needs and to offer their own ideas.

With that, I yield the floor.

The PRESIDING OFFICER (Mr. BOOZMAN). The Senator from Utah.

TRADE PROMOTION AUTHORITY

Mr. HATCH. Mr. President, as the House of Representatives moves closer to a vote on the Senate-passed legislation to renew trade promotion authority, I wish to take a few minutes to talk about the links between our Nation's trade policy, foreign policy, and national security. Whether it is Russia's aggression toward the Ukraine, civil wars in the Middle East or ongoing efforts to prevent nuclear proliferation, the world faces a number of challenges that are impacting the future geopolitical landscape.

In all of this, the question we have to consider is: Going forward, what role will the United States play? Are we going to lead or are we going to follow?

Make no mistake, the path we take on international trade will say a lot about how we plan to answer those questions.

Consider a few facts. In the next few years, China will likely pass the United States as the world's largest economy. It is already the world's largest exporting country. China is continually seeking to expand its influence in order to dictate the terms of international trade, particularly in places like Sub-Saharan Africa, Central Asia, and Latin America.

In other words, when we are talking about trade and the possibility of the United States retreating from the international marketplace, China is the proverbial 800-pound gorilla in the room. Indeed, any ground we cede in leading the world on trade is, more likely than not, ground ceded to China.

I have heard many people—including Members of Congress—express their concerns about China, both strategically and economically, and rightfully so. After all, when it comes to trade, China has constantly shown a disregard for international norms and standards. However, oddly enough, many of those same people who talk the most about the threat posed by China have expressed opposition to TPA, the trade promotion authority bill, and to the Trans-Pacific Partnership or TPP. This is puzzling and reflects a fundamental misunderstanding of the Senate TPA bill and free trade in general.

If we are serious about keeping China and its growing economic and political influence in check, getting a strong TPP agreement that advances U.S. interests should be a top priority. In addition, if we want to eventually convince China to change their harmful practices, a high-standard TPP agreement would naturally be a big step in the right direction.

Free-trade agreements like TPP, if done correctly, should provide new rules for trade in the 21st century. They should set modern standards for economic liberalization and integration, including the protection of foreign investments and intellectual property rights and the marginalization of state-owned enterprises.

We need to be setting the standards and writing the rules on trade so our workers, innovators, researchers, and job creators can fairly compete in the global market. If we don't lead, if we sit on the sidelines, Americans will be competing on an imbalanced playing field, with rules designed specifically to disadvantage us. Given that TPP countries comprise 40 percent of the world economy, it is vital we improve our ability to compete in that region.

Moreover, if TPP fails, we will lose influence in one of the most economically dynamic and strategic regions of the world, and any leadership vacuum left by the United States will almost certainly be filled by someone else and, in this case, most likely China.

But don't just take my word for it. Congress recently received a letter from 17 former Secretaries of Defense and retired military leaders, including Colin Powell, Leon Panetta, William Perry, and Donald Rumsfeld.

In that letter, these leaders said:

We write to express our strongest possible support for enactment of Trade Promotion Authority legislation, which is critical to the successful conclusion of two vital agreements: the Trans Pacific Partnership (TPP) and the Transatlantic Trade and Investment Partnership (TTIP). Indeed, TPP in particular will shape an economic dynamic over the next several decades that will link the United States with one of the world's most vibrant and dynamic regions. If, however, we fail to move forward with TPP, Asian economies will almost certainly develop along a China-centric model. In fact, China is already pursuing an alternative regional free trade initiative. TPP, combined with TTIP, would allow the United States and our closest allies to help shape the rules and standards for global trade.

The concerns outlined in this letter went beyond China.

The letter continues:

The stakes are clear. There are tremendous strategic benefits to TPP and TTIP, and there would be harmful strategic consequences if we fail to secure these agreements. In both the Asia-Pacific and the Atlantic, our allies and partners would question our commitments, doubt our resolve, and inevitably look to other partners. America's prestige, influence, and leadership are on the line. With TPP originating in the Bush administration, these agreements are fundamentally bipartisan in nature and squarely in our national security interest. It is vitally important that we seize the new strategic opportunities these agreements offer our nation.

When 17 former Secretaries of Defense, admirals, and generals who served under both Republican and Democratic administrations have joined together with such a strong message, they probably have a point, and Congress had better listen closely.

Many people, including a number of our colleagues in Congress, continually argue that one of the best uses of American power would be to better promote human rights and democracy in developing countries and increase our efforts at alleviating poverty. I don't necessarily disagree with that sentiment.

Indeed, while there are different opinions about how we can best accomplish these goals, I think most of us in Congress, in both the Senate and the House, agree with the basic premise that we should continually be working to expand our influence and advance our values, particularly in the developing world.

History has demonstrated that the best way to accomplish these objectives is to increase U.S. trade with these countries. Indeed, if we want to export the benefits of American exceptionalism, capitalism, work ethic, and democracy, a freer, expanded exchange of goods is absolutely the best way to do it.

Trade is an effective exercise of America's economic power and influence, trade is how you spread capitalism and encourage other countries to open their economies, trade is how you export American values in the developing world, and, most importantly, trade is how you counter the growing influence of countries like China in the world economy.

The stakes are high. The importance of TPP and other trade agreements to our strategic and security interests is obvious, and given that reality, the importance of TPA should be just as obvious.

Put simply, without TPA, there is no TPP. That is just a fact. Sure, technically speaking, TPA is not required for the administration to complete negotiations and send the agreement to Congress, but technicalities aside, that route is unlikely to yield a desirable result, both in terms of the substance and process.

Japan and Canada, two of our largest trading partners in the TPP negotiations, have each stated they are reluctant to bring their final offers to the table until Congress provides the administration with TPA. Trade promotion authority assures our trading partners that if they reach an agreement, it will not be unraveled when it is sent to Congress for approval. This allows our negotiators to get the best deal possible.

TPA also ensures that Congress has a meaningful role in crafting the specifics of the agreement by setting objectives, mandating transparency, and requiring periodic updates. Under the Senate-passed bill, Congress will have more authority than ever to review and respond to the administration on individual trade agreements.

Long story short, TPA is absolutely necessary for advancing U.S. interests abroad and protecting the opportunities for millions of Americans to earn and compete for a livelihood in an increasingly global trade environment.

With the House TPA vote set to take place in a matter of days, I hope our colleagues in the other Chamber will recognize the strategic and economic realities we face as a country and be willing to advance our Nation's interests and security. I am confident that most of them will make the right choice, and it will be good for America as well as them.

CHILD SUPPORT ENFORCEMENT

Mr. President, I wish to take a few minutes to speak about another matter of great importance not just to me but to everybody.

Last year, after the midterm elections, the Obama administration quietly and without much fanfare proposed a massive, far-reaching rule that would overturn a number of bedrock principles of child support enforcement and welfare reform, chief among them being the principle that parents should be financially responsible for their children.

This was just the latest attempt on the part of the Obama administration to bypass Congress and work to enact policies through executive fiat. Sadly, it wasn't even the first time this administration tried to gut welfare reform. Indeed, we all remember a few years back when the administration granted itself the unprecedented authority to waive critical welfare work requirements.

Put simply, this latest rule would make it easier for noncustodial parents to evade paying child support. It would undermine a key feature of welfare reform, which is that single mothers can avoid welfare if fathers comply with child support orders.

I am fundamentally opposed to policies that allow parents to abdicate their responsibilities, which, in return, results in more families having to go on welfare. I think most Americans would agree with me. That is why I, joined by Senator CORNYN and House Ways and Means Committee Chairman PAUL RYAN, have introduced legislation that would prevent the Obama administration from bypassing Congress in yet another attempt to subvert key features of welfare reform. I regret that we must take this action.

In the past, Members of Congress have generally been able to find common ground and work on a bipartisan basis to address issues relating to child support. In fact, Congress recently passed, and the President recently signed legislation, that made improvements to child support enforcement policies.

In 2013, the Senate Finance Committee reported a series of ambitious proposals related to child support enforcement. At that time, we requested input on these proposals from the Obama administration. At no time did administration officials indicate that the Department of Health and Human Services was quietly working to advance a massive overhaul of child support enforcement, much less that it was planning on doing so without the help or input of Congress.

It is important to note that this secretive preparation only came to light

after the recent elections. That suggests to me that the administration does not have faith that its proposal can withstand public scrutiny and that they have no interest in making a full and transparent justification for the policies they are trying to ram through.

Truth be told, Chairman RYAN and I have introduced our legislation more out of sorrow than anger. For many months, our offices attempted to work out an equitable arrangement with the Obama administration. We tried to convince HHS to withdraw the problematic features of the rule, and in exchange we would agree to engage in a substantive, productive discussion on how to move forward with improvements to child support enforcement.

I firmly believe there is room for common ground. In fact, there are a number of features of the administration's proposed rule that could generate bipartisan support. But any workable solution would have to include the full participation and ultimate consent of the legislative branch. Any changes to the law would have to go through Congress and not simply be dictated by the administration.

So Chairman RYAN and I will do all we can to get our bill through Congress and present it to the President. If we are successful, I hope he will sign it and commit to working with us in the future to advance reforms to child support enforcement. I stand ready to work with the administration and any of my colleagues on both sides of the aisle and both sides of the Capitol to achieve this goal.

Mr. President, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The legislative clerk proceeded to call the roll.

Ms. AYOTTE. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

AMENDMENT NO. 1986

(Purpose: To reauthorize and reform the Export-Import Bank of the United States)

Ms. AYOTTE. Mr. President, on behalf of Senator KIRK, I send an amendment to the desk to the text proposed to be stricken by amendment No. 1463.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from New Hampshire [Ms. AYOTTE], for Mr. KIRK, proposes an amendment numbered 1986 to the language proposed to be stricken by amendment No. 1463.

Ms. AYOTTE. I ask unanimous consent that the reading of the amendment be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

(The amendment is printed in today's RECORD under ''Text of Amendments.'')

Ms. AYOTTE. Thank you, Mr. President.

I rise today to talk about an important amendment that was offered by Senator KIRK, which I cosponsor, and that is the reauthorization of the Export-Import Bank.

I can tell you that in my home State of New Hampshire, on Monday, I was at a roundtable at GE Aviation. GE Aviation has over 700 jobs in the State of New Hampshire. They are building a new facility there. The Export-Import Bank provides a company like GE Aviation the opportunity to obtain financing to export its products that are manufactured in the United States of America, in New Hampshire, to other countries overseas, increasing the opportunity for American manufacturing jobs.

At that company, on Monday, they invited a lot of their suppliers and small businesses who also have either used Ex-Im financing or are suppliers for the larger companies that use Ex-Im financing.

One of those companies that were around the table that had used Ex-Im financing in New Hampshire was Boyle Energy in Concord. In fact, Mike Boyle, who is the CEO of Boyle Energy, has been able to use Ex-Im financing to grow New Hampshire jobs. He has a vision for a new plant in Merrimack, NH, that he is ready to expand. If he can get this financing, he is going to be selling more of his great products overseas, creating more jobs in New Hampshire.

Yet, this Bank expires at the end of June. This is a very important tool for American businesses. This program—and I wish I had this problem with every program in Washington—actually returns money to the Treasury, and it creates American jobs.

The reason this type of financing is available is because of the risk that is often taken in exporting products and there aren't commercial loans always available. The Ex-Im Bank has the ability to allow financing for our businesses in America. In fact, other countries around the world have programs such as this, and that are much more extensive. So without the Ex-Im Bank, it is not a level playing field for our American companies that want to manufacture in the United States of America. The Ex-Im Bank will allow access to financing that will enable businesses to create American jobs.

Also around that table on Monday at GE Aviation was Goss International. They manufacture great printing presses in New Hampshire. We are very proud of them. They have also been able to use Ex-Im financing. If that financing doesn't go through, we heard from a representative of Goss that, in fact, they could lose up to 40 jobs in my home State of New Hampshire. So it is important that we reauthorize this Bank.

I want to thank the Senator from Illinois for offering this amendment to reauthorize the Ex-Im Bank so that our companies here in the United States of America can manufacture here, sell to consumers around the world, and have access to this financing. In fact, in New Hampshire there have been about 36 companies—many of them small companies—that were able over the last several years to use Ex-Im financing to create New Hampshire jobs.

This is about jobs in the United States of America. This is about competing. We recently had the TPA—trade promotion authority—on the floor to expand opportunities for trade. This goes hand in hand with that legislation so that companies have opportunities to get financing to create jobs here and return money to the Treasury. I wish I could say that about every program—that it returns money to the Treasury. The default rate at Ex-Im Bank is lower than with commercial loans.

I hope that Senator KIRK's amendment will get a vote on the Senate floor, that we can get this reauthorized before the expiration date at the end of this month, and that we can continue to allow this financing for American businesses to continue to build and create products to sell overseas and to create American jobs. This is what this financing allows these businesses to do. This is very important in making sure that we remain competitive and that we have more jobs here and that we continue to sell our great products built here in the United States of America around the world.

So I am very honored to support this amendment. I hope we will get a vote on this amendment on the Defense authorization bill or get a vote and make sure that we have this passed before the end of this month when this Bank expires so that we could have continuity in this important financing mechanism for our businesses here in this country.

In addition to the businesses I previously mentioned that were around the table on Monday, I also want to mention GKN Aerospace from Charleston, which is a larger business with a smaller footprint in New Hampshire that has been able to export and create jobs in New Hampshire and across the country. In addition to that, we were so glad to hear from other businesses in New Hampshire that were able to rely on this important financing mechanism.

I am very glad to support Senator KIRK's amendment.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Florida is recognized.

SPACE PROGRAM CUT

Mr. NELSON. Mr. President, I just learned that the CJS subcommittee of the Appropriations Committee reported a bill out that made a substantial cut in the request for commercial crew in order for us to be able to have Americans flying on American rockets to and from the International Space Station, instead of having to rely on the Russian Soyuz, which we buy and have been buying those ever since we shut down the space shuttle at something like $60 million to $70 million per

passenger going up to the space station.

Now, the whole idea was that since we cooperated with the Russians in building this space station, we would both have the means of transportation to get up there. We do have the means of transportation of getting cargo to and from the space station, since we shut down the space shuttle, but we are in the process of a competition between several companies—especially those that have been selected in the competition by NASA, Boeing and SpaceX. Each of them has been granted money to develop all of the redundancies and safety and escape systems in their spacecraft capsule in order to make it safe for Americans to go to and from the International Space Station.

Now, I can tell you that for the average American on the street, their image of our space program is one that since the space shuttle shut down in 2011, they think the space program is over, when, in fact, it is really just beginning, and we are going to Mars in the decade of the 2030s. Well, that is the whole point of our being able to rely on our own spacecraft and on our own rockets, instead of relying on the Russians.

If this cut is sustained—and this is a cut from a request of $1.24 billion for this competition for making American rockets safe and creating the spacecraft to take Americans to the space station—it will have been cut to $900 million. If that cut in the subcommittee is sustained in the full committee and ultimately in the final appropriations bill, it is going to delay us from being able to launch Americans on American rockets.

Instead of 2017—just 2 years from now—it will delay us another 4 years. That is 4 more years of relying on the Russians. Now, I know there are a bunch of Senators around here that do not like the fact of the aggressiveness of Vladimir Putin. Well, this is one way to wean ourselves from having to depend on them.

The final comment on this subject is that the money that supposedly is being cut, which is just a little over $300 million, we would lose in still paying that money to the Russians to fly an additional 2 years. We need to wake up to what is happening. Senator MIKULSKI will be offering an amendment to the full Appropriations Committee to restore that cut. I hope Senators will understand all the nuances and support Senator MIKULSKI.

I yield the floor.

The PRESIDING OFFICER (Mr. GARDNER). The Senator from Illinois.

AMENDMENT NO. 1986

Mr. KIRK. Mr. President, I seek to speak on my amendment on behalf of the Export-Import Bank. I would like to say the Export-Import Bank is set to expire this year on June 30. It allows thousands of American companies to advance their technology overseas. Without these loans, many American jobs would be ceded to China or Europe.

Now, 200,000 American workers depend on Ex-Im, plus 46,000 in my home State of Illinois. They work for these companies that depend on Ex-Im's backing to make exports happen. Some people are interested in killing this agency because it may be a government handout agency. It is not. It actually makes the taxpayer $1 billion a year. In the last 3 years, it has earned the U.S. Treasury over $3 billion.

I will be offering the Kirk-Heitkamp amendment to keep this Bank alive. I want to thank Senators BLUNT, CANTWELL, and MANCHIN for defending these American jobs.

I yield the floor.

The PRESIDING OFFICER. The Senator from North Dakota.

Mr. HOEVEN. Mr. President, I rise to speak about the National Defense Authorization Act. This is legislation we are currently considering that we need to pass. It is important for our military, and it is important for the American people. I have offered a number of amendments, and I rise to speak about three of those amendments at this point.

The first is amendment No. 1483, which involves RPA flight training. Essentially, amendment No. 1483 would instruct the Air Force to consider allowing private contractors to provide the Air Force with training for remotely piloted aircraft or RPAs. These are the vehicles used in unmanned aerial systems, commonly called UAS.

Currently, the Air Force is training pilots for RPAs, remotely piloted aircraft, within the service itself. But there are some very skilled private contractors. In fact, the people who make unmanned aircraft could be doing high-quality training for them as well, particularly in concert with our universities that provide aviation training.

Right now the Air Force faces a real challenge in training a sufficient number of unmanned aircraft pilots to meet operational demands. Specifically, this amendment directs the Air Force to evaluate the use of private contractor facilities, equipment, and trainers to increase the number of qualified pilots for our RPA missions. It requires the Air Force to detail various aspects of their shortfall in manning RPAs, the authorized number of personnel assigned to the missions, and the identification and assessment of actions to address that shortfall.

In this rapidly growing era of unmanned aerial systems technology, it just makes sense for the military to partner with companies and universities that have the expertise to provide the critical training the military needs. It is cost effective. It is efficient. It is good for the military and our country. Right now the demand for unmanned aerial systems is so strong worldwide that the Air Force has all of its pilots flying the missions. That does not give them the resources, the pilots to train more pilots to fly unmanned aerial systems.

So this is a way that we can help the Air Force train these new pilots with the very contractors that make things such as Global Hawk, Predator and with our universities that provide aviation training. I think it would be of great benefit and assistance to the Air Force.

The second amendment that I want to talk about is amendment No. 1484. This one seeks to give the Air National Guard units a larger role in the Global Hawk unmanned aerial systems mission. Specifically, this measure directs the Air Force to determine the feasibility of partnering the Air National Guard with Active-Duty Air Force to operate and maintain the Global Hawk. The RQ–4 Global Hawks, including the Block 20, Block 30, and Block 40 variants, are the Air Force's high-altitude, long-endurance aircraft for intelligence, surveillance, and reconnaissance.

They are currently operated and maintained only by Active-Duty forces. But the Air National Guard could be providing a valuable adjunct to the Air Force's regular personnel if we allow them to do that. The North Dakota Air National Guard, for example, already operates and maintains the armed MQ–1 Predator, and does it exceptionally well. They and units like them are clearly capable of taking on part of the Global Hawk mission, in association with their Active-Duty counterparts.

This amendment would further the joint operations which have been a major initiative of all of the armed services, the Guard, and the Reserves in recent years, and they have done a tremendous job on jointness. It has made our military stronger, more effective, and more responsive. We need to continue to build on that joint operation. That is exactly what this amendment does.

The third amendment that I would like to discuss is amendment No. 1485. It regards the Nuclear Force Improvement Program. This amendment seeks to fortify the Nuclear Force Improvement Program, or NFIP, which I believe is crucial to our national security both now and well into the future. The reality is that we are facing an increasingly nuclearized future. Nations such as Iran, North Korea, and others have or are developing nuclear weapons.

That means we must maintain a credible, decisive nuclear deterrent. That is what the Nuclear Force Improvement Program is all about. In 2014, the Air Force initiated the program to bolster and enhance its nuclear missions, including the intercontinental ballistic missile, ICBM, and nuclear-capable bomber missions. The program involves a wide range of efforts to improve morale, update facilities and equipment, and reinvigorate the nuclear-related career fields in the Air Force.

We need to continue to invest in and build this program. Specifically, my amendment provides that the nuclear mission should be a top priority for the

Department of Defense and the Air Force; that Congress should support investments which sustain progress made under the Nuclear Force Improvement Program; that the Air Force should regularly inform Congress on the program's progress and any additional requirements it may identify; and that future Air Force budgets should reflect the importance of the nuclear mission and the need to support personnel performing the nuclear mission.

The bottom line is that the men and women assigned to the nuclear mission in the U.S. Air Force are doing incredibly important work every day for the security of our country. We need to do all we can to support them. We need to provide them with the support they deserve so they can continue to do the job we ask them to do and do it at the level that our security requires.

The Nuclear Force Improvement Program is a success, and the Air Force needs to extend it into the future and continue to shore up the foundations of our nuclear deterrent, which is, itself, at the foundation of national security.

In conclusion, let me say that working on legislation as essential as the defense of our Nation is and should be a bipartisan effort. The Senate Armed Services Committee passed this bill out of committee with a bipartisan vote of 22 to 4. Let's come together and do this for the American people and the men, women, and families who have undertaken the great and noble effort to protect our country.

I want to thank both the chairman of the Armed Services Committee and the ranking member for their hard work, for their bipartisanship, and, again, offer my support as we work to pass this vitally important legislation for our military and for this great country.

I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The bill clerk proceeded to call the roll.

Mr. DONNELLY. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. DONNELLY. Mr. President, I wish to tell you a little bit about Gregg Keesling, a dad and small business owner from Indianapolis. I have gotten to know Gregg over the past few years because Gregg and his wife Jannett lost their son Chancellor to suicide while Chancellor was serving in Iraq in 2009, joining a club he often says he doesn't want anyone else to join.

On the poster, this is Gregg and this is Chancellor. This is Chancellor again, on duty. This is the memorial they had for Chancellor.

Gregg recently said that he sees the invisible wounds borne by our men and women in uniform as ''one of the greatest challenges that our country faces.'' And he noted that ''we're going to face this challenge for many years to come.'' Gregg is right. We have lost more troops to suicide than in combat each of the past 3 years. We lost more than 400 Active-Duty, Guard, and Reserve servicemembers last year alone. It is also estimated that we lose 22 veterans to suicide every single day. These are preventable deaths.

We must do more to get these men and women the mental health care they have earned. We need to remind our troops and veterans, along with our friends and family, that it is OK to share the burden of their personal struggles. It is a sign of strength to seek help. Our servicemembers, veterans, and their families sacrifice for us, so we must do everything possible to support them.

Last year we passed and the President signed into law the Jacob Sexton Military Suicide Prevention Act, which for the first time requires an annual, in-person mental health assessment for all servicemembers, whether they are Active, Guard, or Reserve. Just like physical health, mental health is an essential piece of military readiness. We need to have an attitude of all-in toward providing support for mental health challenges and also for the day-to-day struggles we know contribute to suicide risk, such as financial problems, relationship issues—things that are never made easier by military life.

The Sexton act was named for a member of the Indiana National Guard who took his own life while home on leave from Afghanistan in 2009. Jeff and Barb Sexton, Jacob's parents, have been incredible partners in this work. Jeff recently spoke about the decision he and his wife made to speak out about military suicide.

This is SPC Jake Sexton. Here he is in his Humvee, and here he is serving as well. His parents, Jeff and Barb—actually, it was Jeff in particular, his dad, who said:

I had three choices: I could crawl in a corner, I could crawl in a bottle or I could stand up and fight. It's not been an easy job, but it's something I feel me and my wife have to do.

The Keeslings and the Sextons are courageously telling their stories to help prevent any more families from going through this nightmare. Congress needs to continue to answer their call. This is an issue we cannot let up on because there is so much more important work to do.

This year, we are taking the next step in the continuum of care and focusing on improving the quality of and access to mental health care through Department of Defense providers, VA providers, and private community providers.

This year, we introduced the servicemember and veteran mental health care package—three bills. Each improves access to quality mental health care for servicemembers and veterans. The care package aims to improve mental health care by focusing on direct care providers at DOD and VA, community providers in their own towns, and the training of physician assistants as mental health providers.

I thank Chairman MCCAIN and Senator REED for working with me to include elements of the care package in the national defense bill, specifically those elements which deal with DOD and care for servicemembers.

I wish to go through the care package provisions in the NDAA briefly and offer two amendments to ensure that these provisions support not only servicemembers but also veterans.

First, section 716 is based on the first of our care package bills, the Community Provider Readiness Recognition Act. It is cosponsored by my friend, Senator JONI ERNST, and it creates a special military-friendly designation for providers who choose to receive training in military culture and the unique needs of servicemembers and military families. Providers who receive this designation would be listed in a regularly updated online registry, allowing servicemembers to search for designated providers in their area.

This bill is inspired by the Star Behavioral Health Provider Network, which is a program that the Military Family Research Institute at Purdue University built in Indiana to train providers to better understand military culture and medical treatments. Designating a provider as part of the Star Behavioral Health Provider Network helps servicemembers and their families make informed choices about where to seek care. This can easily be translated on a national scale so that servicemembers, veterans, and their families know which private mental health care providers are well-suited and trained to treat them.

Mr. President, second, section 713 of the NDAA is drawn from another care package bill, the Military and Veterans Mental Health Provider Assessment Act, cosponsored by my friend Senator ROGER WICKER of Mississippi.

This legislation requires that all of DOD primary care and mental health providers have received evidence-based training on suicide risk recognition and management and that their training be updated to keep pace with changes in mental health care best practices.

It also requires DOD to report to Congress on the military's current mental health workforce, the long-term mental health needs of servicemembers and military families, and how we ensure DOD meets those needs.

Finally, it requires the Department of Defense to bring us a plan to assess mental health outcomes in DOD care, variations in outcomes across different DOD health care facilities, and barriers to DOD mental health providers implementing the best clinical practice guidelines and other evidence-based treatments.

Finally, by including elements from the Frontline Mental Health Provider Training Act, cosponsored by my friend Senator JOHN BOOZMAN from Arkansas, the NDAA calls on the Department of

Defense to train physician assistants to specialize in psychiatric care in order to help meet the increasing demand for mental health services among servicemembers and their families. We are also working to extend the same spectrum of care to our veterans, and we are working toward a hearing on the corresponding veterans bills for this mental health care package in the months ahead. These are smart, bipartisan provisions that address one of the most serious challenges facing our military, our veterans and our country.

We must improve the mental health care at the Department of Defense and the Veterans' Administration and at private community providers from Ellsworth, ME, to Evansville, IN, to the shores of California so they are better able to serve our servicemembers, veterans, and their families. It is absolutely essential that we have coordination and continuity for servicemembers and their families as they transition to veteran status.

I will leave you with a couple of brief thoughts from two brave Hoosiers I have the privilege to know and have gotten to know well. Jeff Sexton, Jacob's dad, put it this way: ''It is one thing to lose someone you love in the war. It is a whole other thing to lose them to the war.'' And Gregg Keesling, Chancellor's dad, concluded this: ''The bottom line is I don't want anybody to go through what we've gone through.''

We must act and we must act now before any more families have to experience this loss from suicide. I urge all of my colleagues to support the care package provisions for servicemembers and to later extend them to our veterans who need our help and who need us to stand up for them.

Mr. President, I yield the floor.

I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. MURPHY. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. MURPHY. Mr. President, I am coming to the floor to speak on behalf of an amendment I am offering, along with Senators SCHATZ, UDALL, BLUMENTHAL, HEINRICH, TESTER, MERKLEY, and BALDWIN.

Today, it was announced that President Obama is going to be sending another 450 troops to Iraq to help assist in the fight against ISIL. That will mean we now have 3,500 troops in position throughout Iraq assisting in the battle against ISIL within those borders. This marks also nearly a year since we have reengaged in military activities in Iraq and in Syria, both with support forces for the Iraqis, with training for those who are fighting in Syria, and major air operations targeting ISIL.

I think there is broad bipartisan consensus here that the United States needs to take the fight to this enemy—an enemy that is seeking to occupy an enormous amount of territory in a very dangerous region from which it can plot attacks against the United States. But I also think there is bipartisan agreement that we should do our constitutional duty; that we should authorize this war against ISIL. My hope is the Foreign Relations Committee—of which I am a member, of which the Presiding Officer is a member—will have that debate in the upcoming months.

But given that we are authorizing hundreds of millions of dollars in this bill in order to take the fight to ISIL, I think it makes sense to have some commonsense limitations on the use of that money that are in keeping with the very public promises the President has made.

President Obama has stated very clearly that he does not think it is a wise strategy to reinsert major combat troop operations into the Middle East. I agree with him. I think many of us agree with him. There is nothing about the last 10 years of American occupation in Iraq that tells us that U.S. troops inside Iraq can have the effect of killing more terrorists than are created, in part, through the recruitment benefit of major U.S. combat operations.

So the amendment we are offering today is a fairly simple one. It would prohibit the use of major combat—of large numbers of combat troops in the fight against ISIL, with certain commonsense exceptions: an exception for rescue operations, an exception for intelligence-gathering exercises, and an exception for special operations in and throughout the region; special operations like the one we used to kill a high-ranking ISIS commander just within the last several weeks.

We think it is important that Congress weigh in and state what we believe to be the desire and imperative of our constituents; that we learn from the mistakes of the Iraq war; that we don't repeat them by inserting thousands of American ground troops back into Iraq or perhaps Syria.

ISIS was created, first and foremost, primarily by a political vacuum inside Iraq, not a military vacuum. We need to acknowledge that any strategy to ultimately defeat ISIL, as we are all committed to, has to first and foremost have a realistic political strategy on the ground to divorce Sunni populations from this death cult that is ISIL.

Sunni grievances grew throughout Nouri al-Maliki's reign. They were denied an equitable share of oil revenues. They were excluded from government jobs. There were real atrocities committed against Sunni communities—mass incarcerations, torture, extrajudicial killings. If we don't have an Iraq Government that is committed to being inclusive of Sunni populations, there is no amount of American troops on the ground that can heal those divisions. In fact, what we know about the Iraq war is that major American combat operations on the ground in Iraq have an effect of exacerbating those divisions rather than healing them. They give space for people like Maliki to try to marginalize these populations. They increase suffering on the ground, especially for these populations that aren't represented effectively within the reigning Shiite government in Baghdad.

So if we really want to learn lessons from the past, then let's take President Obama at his word. Let's include in the NDAA a commonsense limitation, with exceptions, with respect to the deployment of major ground operations inside Iraq.

Now, there are some people who will say this isn't the role of Congress. I would just state for the record that there are a litany of examples in the past in which Congress has placed commonsense limitations on our authorizations for military force. In fact, the President, in submitting a proposed AUMF to the Foreign Relations Committee several months ago, in fact, included in that authorization of military force a limitation on ground forces. So this would be entirely consistent with the history of this body but also with the proposal the President has made.

I know, from having visited our troops in Iraq and in Afghanistan, that it is easy for us to believe there is no mission that U.S. soldiers can't take on; that their capability, that their bravery, that their courage, that their adaptability knows no bounds. They have done admirable work inside Iraq over the course of the last 10 years, but what we know is that those troops inside Iraq also made Iraq what our own intelligence community called the cause celebre for the international terrorist movement, drawing in thousands of would-be terrorists to fight the Americans.

What we know is that the ISIS we are fighting today is a follow-on organization from Al Qaeda in Iraq, which was created because of the American invasion and occupation—maybe not in whole but certainly as the primary influence.

So we hope to be able to have a full debate on an authorization of military force. But with the inability to move that piece of legislation through the Foreign Relations Committee, we think it is proper on the NDAA to hold the President at his word, place a commonsense limitation on the use of ground troops and learn from the mistakes of the last 10 years inside Iraq.

I yield the floor.

The PRESIDING OFFICER. The Senator from Illinois.

AMENDMENT NO. 1986

Mr. KIRK. Mr. President, I urge this Chamber to reject the motion to table my amendment, which put forward reforms to the Export-Import Bank. I would say to Members that this is going to be a key scored vote by the

U.S. Chamber of Commerce and the National Association of Manufacturers; that, without my amendment, we would not have the reforms to make sure Ex-Im works at least 25 percent of its portfolio with small businesses.

I urge Members to vote no on the motion to table my amendment by Mr. SHELBY that I understand is coming up. This is a key test vote, Export-Import Bank. With a good bipartisan vote, I would think we would have people supporting the Kirk-Heitkamp-Blunt-Graham reform legislation for Ex-Im.

I yield the floor.

Mr. SHELBY. I suggest the absence of a quorum.

The PRESIDING OFFICER. The clerk will call the roll.

The senior assistant legislative clerk proceeded to call the roll.

Mr. GRAHAM. Mr. President, I ask unanimous consent that the order for the quorum call be rescinded.

The PRESIDING OFFICER. Without objection, it is so ordered.

Mr. GRAHAM. Mr. President, very briefly. Senators AYOTTE and KIRK's amendment is coming up. There will be a motion to table. What we are trying to do is basically show support for the Ex-Im Bank, which is due to expire in June. We are trying to find a vehicle, a must-pass piece of legislation, to keep the Bank afloat. I think it is very important to the American economy that American manufacturers not be disadvantaged. The Ex-Im Bank makes money for the American taxpayer. China's Ex-Im Bank is larger than France, Germany, the United States, and England's combined.

What does this mean to the average person? When a product is made in the United States and sold into the developing world without the Ex-Im financing mechanism available to American manufacturers, we are going to lose market share to other countries like China, France, Germany that produce wide-body jets and other products. Eighty-nine percent of the people who get help from the Ex-Im Bank are small businesses.

This is an attempt to show the investor community and those who are watching this issue that the Senate is in support of the Bank. So I am urging a ''no'' vote on tabling. We had to do this procedurally. So this will be a signal to the markets that the Senate is in support of the Bank. I urge everyone who believes the Bank is vital to American exports and not against unilateral surrendering of market share to the Chinese and other competitors to vote no. There will be another vote of our choosing on a vehicle that will have to get to the President's desk. This is not the last vote we will take on Ex-Im Bank.

I yield the floor.

The PRESIDING OFFICER. The Senator from Kansas.

Mr. MORAN. Mr. President, I understand we have a vote scheduled at 5 o'clock, and I appreciate the opportunity to speak for about 60 seconds.

AMENDMENT NO. 1473

I came to the floor today to speak in favor of an amendment described earlier in the afternoon by Senator VITTER. This is an amendment, of course, to the National Defense Authorization Act that makes certain our U.S. Army is able to maintain the current number of brigade combat teams.

Sequestration is creating significant problems in many arenas but no more important than in the area of our Army and defense. The concern is that in the process of downsizing the Army as a result of sequestration and other reductions in available funding, brigade combat teams would be eliminated. Senator VITTER's amendment, which I support and am a cosponsor of, would eliminate that as an option.

The PRESIDING OFFICER (Mr. LEE). The Senator from Alabama.

AMENDMENT NO. 1986

Mr. SHELBY. What is the pending business?

The PRESIDING OFFICER. It is the Ayotte-Kirk amendment.

Mr. SHELBY. Mr. President, I rise today in opposition to the amendment, which is a long-term reauthorization of the Export-Import Bank. In my opinion, after evaluating this issue during a series of hearings in the Senate banking committee, there is no compelling case to reauthorize the bank.

After years of efforts to reform the Export-Import Bank, it has become clear to me that its problems are beyond repair and that the Bank's expiration is in the best interest of American taxpayers. Nearly 99 percent of all American exports—over $2 trillion—are financed without the Export-Import Bank's help, which demonstrates that the subsidies are more about corporate welfare than advancing our economy.

I believe the Export-Import Bank has outlived its usefulness and should be allowed to expire.

At this point, I move to table the Kirk amendment No. 1986 and ask for the yeas and nays.

The PRESIDING OFFICER. Is there a sufficient second?

There appears to be a sufficient second.

The question is on agreeing to the motion.

The clerk will call the roll.

The senior assistant legislative clerk called the roll.

Mr. CORNYN. The following Senators are necessarily absent: the Senator from Florida (Mr. RUBIO) and the Senator from Pennsylvania (Mr. TOOMEY).

Mr. DURBIN. I announce that the Senator from Oregon (Mr. MERKLEY) and the Senator from Nevada (Mr. REID) are necessarily absent.

The PRESIDING OFFICER. Are there any other Senators in the Chamber desiring to vote?

The result was announced—yeas 31, nays 65, as follows:

[Rollcall Vote No. 206 Leg.]

YEAS—31

Barrasso	Fischer	Risch
Boozman	Flake	Sanders
Capito	Gardner	Sasse
Cassidy	Grassley	Sessions
Corker	Inhofe	Shelby
Cornyn	Isakson	Sullivan
Cotton	Lankford	Thune
Crapo	Lee	Tillis
Cruz	McConnell	Vitter
Daines	Paul	
Enzi	Perdue	

NAYS—65

Alexander	Franken	Murkowski
Ayotte	Gillibrand	Murphy
Baldwin	Graham	Murray
Bennet	Hatch	Nelson
Blumenthal	Heinrich	Peters
Blunt	Heitkamp	Portman
Booker	Heller	Reed
Boxer	Hirono	Roberts
Brown	Hoeven	Rounds
Burr	Johnson	Schatz
Cantwell	Kaine	Schumer
Cardin	King	Scott
Carper	Kirk	Shaheen
Casey	Klobuchar	Stabenow
Coats	Leahy	Tester
Cochran	Manchin	Udall
Collins	Markey	Warner
Coons	McCain	Warren
Donnelly	McCaskill	Whitehouse
Durbin	Menendez	Wicker
Ernst	Mikulski	Wyden
Feinstein	Moran	

NOT VOTING—4

Merkley	Rubio
Reid	Toomey

The motion was rejected.

The PRESIDING OFFICER. The Senator from New Hampshire.

AMENDMENT NO. 1986 WITHDRAWN

Ms. AYOTTE. Mr. President, on behalf of Senator KIRK, I withdraw amendment No. 1986.

The PRESIDING OFFICER. The Senator has that right. The amendment is withdrawn.

CLOTURE MOTION

Mr. MCCONNELL. Mr. President, I send a cloture motion to the desk for amendment No. 1569, as modified.

The PRESIDING OFFICER. The cloture motion having been presented under rule XXII, the Chair directs the clerk to read the motion.

The legislative clerk read as follows:

CLOTURE MOTION

We, the undersigned Senators, in accordance with the provisions of rule XXII of the Standing Rules of the Senate, do hereby move to bring to a close debate on amendment No. 1569, as modified, to the McCain amendment No. 1463 to H.R. 1735, an act to authorize appropriations for fiscal year 2016 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.

Mitch McConnell, Lamar Alexander, John Cornyn, Orrin G. Hatch, David Perdue, Bob Corker, Michael B. Enzi, Susan M. Collins, Jeff Flake, Mike Rounds, Richard Burr, David Vitter, James M. Inhofe, Daniel Coats, John McCain, Deb Fischer, Tom Cotton.

Mr. MCCONNELL. I ask unanimous consent that the mandatory quorum required under rule XXII be waived.

The PRESIDING OFFICER. Without objection, it is so ordered.

The Senator from North Dakota.

Mr. COATS. Will the Senator yield for a unanimous consent request?

Ms. HEITKAMP. Sure.

MORNING BUSINESS

Mr. COATS. Mr. President, I ask unanimous consent that the Senate proceed to a period of morning business, with Senators permitted to speak for up to 10 minutes each.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

Mr. COATS. I thank the Senator.

The PRESIDING OFFICER. The Senator from North Dakota.

AMENDMENT NO. 1986

Ms. HEITKAMP. Mr. President, I am very excited about the Kirk-Heitkamp amendment getting an overwhelming show of support. The reality is that if we do not vote on the Kirk-Heitkamp bill itself and pass it out of this Chamber, at the end of this month, the charter for the Ex-Im Bank will expire.

This vote has nothing to do with the charter for the Ex-Im Bank. It does nothing to prevent the charter for the Ex-Im Bank from expiring. This is at a time when China and India are pumping billions of dollars into their export credit agency. This is at a time when we have $15 billion worth of credit waiting to move through the Ex-Im Bank so we create jobs here in our country—jobs for American workers—and we are stalling the Bank.

When we had this discussion during the TPA debate, we wanted to have a vote that would guarantee we would have an opportunity to prevent the charter for the Ex-Im Bank from expiring. That is not this vote today.

I am extraordinarily gratified by the show of support because what it really does tell us is if we bring up an Ex-Im Bank bill on its own—an extension bill on its own—we will be able to prevent something from happening that could have catastrophic economic results in this country. So I urge this body to find a path forward to prevent the Ex-Im Bank charter from expiring, to have a path forward to honor our commitments that were made during an earlier vote so we can have a vote and actually move this bill forward and not simply have a vote to show support but actually pass a bill.

Mr. DURBIN. Mr. President, will the Senator from North Dakota yield for a question?

Ms. HEITKAMP. Yes.

Mr. DURBIN. I thank the Senator for her comments and I ask her this question: So that we understand the procedure that just took place, there was an amendment offered that would have extended the Ex-Im Bank and then a motion to table it, and I believe 60 Members or more voted against the motion to table, which shows a positive sentiment about extending the Ex-Im Bank charter. After that vote, the sponsors of the amendment withdrew the amendment from this bill.

So at this moment in time, I wish to ask the Senator, for absolute clarity: We have nothing before us that would extend the Ex-Im Bank either in this bill or in any other manner before the end of June when it expires; is that correct?

Ms. HEITKAMP. That is absolutely correct.

Mr. DURBIN. And that creates a disadvantage for businesses in Illinois, and I am sure in North Dakota, in terms of exports and jobs, and unless we do take this seriously and quickly, they will be jeopardized.

Ms. HEITKAMP. I think the other thing it does also is it is a signal to all of those companies we are competing with, whether it is China or India, that we are out of the business, and that opens a wide path for them to be in the business of exports. So this takes us out of the business of financing exports, which is going to have and will have catastrophic results. We don't have a path forward, and the charter of the Bank expires at the end of this month. Without a path forward, we are opening an opportunity for our competitors to take those exports and to take away our opportunity to have those jobs.

So I am very gratified by the result of this vote because I think it signals support for Ex-Im Bank. When we get this kind of support from the U.S. Senate—almost veto-proof support—maybe we ought to move the bill. People will say there isn't an opportunity to do that; there is no path forward. Let me tell my colleagues that there is no one in the country who believes that is true. If there is a will, there is a way.

We have to have a vote on the Export-Import Bank by the end of the month and get it over to the House so the House can support it and move this forward or we will be playing chicken with the exports of the United States of America.

Mrs. SHAHEEN. Will the Senator yield for another question?

Ms. HEITKAMP. Yes.

Mrs. SHAHEEN. Senator AYOTTE, in offering this amendment, talked about a forum in New Hampshire at General Electric where a number of small businesses participated. Senator CANTWELL and I were at that forum. We heard testimony from an employee of a company called Goss International, which makes large printing presses and competes mostly with Germany but with countries around the world. One of the issues she spoke about is that they have $10 million in deals that are sitting on the table at Ex-Im that they need to have approved before the end of June when the authorization expires. If those don't get approved, they are not going to be able to create 45 new jobs they are talking about being able to create as part of that deal.

So if the authorization for Ex-Im expires, not only is Goss going to have trouble with those jobs, but companies across this country are going to lose jobs that would be created if those financing deals could go through; isn't that the case?

Ms. HEITKAMP. In fact, the case is nearly $16 billion worth of American business and American exports that create American jobs will languish in the pipeline at the Ex-Im Bank because we foolishly let a charter expire at a time when we are in competition for exports, a competition for commerce throughout the world.

When we debated trade promotion—and a lot of us took some tough votes on TPA—we were promised a vote that would be mutually agreed upon here so we could advance the Ex-Im Bank by the end of June. We haven't gotten that vote because today all we did was show—I think rightfully so—that we have tremendous support in this body for the Ex-Im Bank and we shouldn't be held hostage to the narrow ideology of a few.

Ms. CANTWELL. Mr. President, will the Senator yield for a question?

Ms. HEITKAMP. Yes.

Ms. CANTWELL. The Senator from North Dakota has obviously been working so hard on this in the Banking Committee, and she understands, I believe, that when the Bank expires on June 30, there is about $12 billion of approved deals that are in the process, and they will not be approved while the Bank is not operating; is that correct?

Ms. HEITKAMP. That is correct. The last number I was given, I say to my friend, the Senator from Washington, was almost $5.5 billion.

Ms. CANTWELL. So today's vote is a symbolic vote but does nothing to help us resolve the issue for getting this approved before June 30.

Ms. HEITKAMP. Unfortunately, too often we have symbolic votes that don't have real consequences in the real world. Our wonderful businesses that are outcompeting and outmanufacturing and outdeveloping and outresearching the rest of the world are now with their hands tied behind their backs and losing credits as we stand.

Ms. CANTWELL. Are there a lot of small businesses in South Dakota that are a part of this export economy?

I say that because I think a lot of people get the impression that this is about big manufacturers. I have always said those guys will take care of themselves; they have lots of people here to take care of them. But the small people who will actually lose business on June 30 don't have people here and that is why we are fighting so hard to get a vote before June 30 that actually will go over to the House on a vehicle.

Ms. HEITKAMP. We have companies in Wahpeton, ND, where bankruptcy has been prevented because they have been able to find their way to the Ex-Im Bank and actually find their way to a credit relationship with their importers.

We have a company in West Fargo that builds portable wheelchair ramps and they have saturated the market here and they are marketing these all