to Blair's charade. The IG allowed it to go on and on. Countless man-hours and millions of dollars were wasted on cooking the books and on vicious infighting instead of productive problem-solving to right the ship. Mr. Coleman and the GAO got that done.

On March 23, the day before the IG's final exit briefing with the GAO, came a bolt from the blue. The IG stepped forward with a brave, bold announcement. The clean opinion was formally withdrawn. It was like a rush of fresh air in a very stuffy room. The inescapable truth finally dawned on Inspector General Rymer. So I want to thank Mr. Rymer for having the courage to do the right thing.

An audit failure of this magnitude should have consequences. This one is especially egregious. It leaves at least one former Secretary of Defense with egg on his face. Mr. Blair was removed as head of the Audit Office on June 10 but is still serving as the Office of Inspector General's Deputy Chief of Staff. He is the chief architect of the now discredited clean opinion. He is the one who planted the seeds of destruction when he allegedly quashed the audit team's disclaimer. Of course, those responsible for what happened ought to be held accountable.

Mr. Blair wants us to believe that the muffed opinion was the result of a routine dispute between opposing auditors' judgments over evidence, a mere difference of opinion among auditors. True, it reflects an unresolved dispute between the audit team and the management, and yes, that happened; however, there is a right way and a wrong way to resolve the conflicts.

The PRESIDING OFFICER. The Senator's time has expired.

Mr. GRASSLEY. Mr. President, I ask unanimous consent to complete this. I was told I would be given the time to do it, and I have about 4 minutes.

The PRESIDING OFFICER. Is there objection?

Mr. SANDERS. Mr. President, reserving the right to object, and I won't object, I want to make certain that after Senator GRASSLEY has completed his remarks, I will have time to make my remarks for up to 15 minutes. It will probably be less than that.

Is that all right, Senator?

Mr. GRASSLEY. That is OK.

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

Mr. GRASSLEY. Those responsible for what happened ought to be held accountable.

Mr. Blair wants us to believe the muffed opinion was the result of a routine dispute between opposing auditors' judgments over evidence and a mere difference of opinion among auditors. True, it reflects an unresolved dispute between the audit team and management, and yes, that happened; however, there is a right way and a wrong way to resolve such conflicts. According to audit standards cited in the GAO report, the dispute should have been addressed, resolved, and documented in workpapers before the report was issued. It was not because the two opinions were irreconcilable.

The team's disclaimer was based on evidence measured against standards documented in workpapers. Blair's so-called ''professional preference,'' by comparison, is none of these things. As the GAO's evidence gap suggests, Mr. Blair's opinion was hooked up to nothing. It was unsupported, and it was improper. So plain old common sense should have caused senior managers to realize that issuing the report with the opinion hanging fire was a senseless blunder. Doing it had one inevitable result: The opinion had no credibility, and that opinion had to go.

True, the integrity of the Office of Inspector General audit process may be damaged, but the final outcome of this tangled mess may help clear the way for recovery. That recovery ought to lead us to being able to have clean audits not only of the Marine Corps but all of the four services. The Marine Corps audit was the first big one out the box. If Inspector General Rymer had not embraced the truth, we might be staring at a bunch of worthless opinions awarded to the Army, Navy, and Air Force. The Department of Defense could have declared victory and buried the broken bookkeeping system for another 100 years.

Hopefully, the Defense Department will begin anew with fresh respect for the truth, audit standards, and the need for reliable transaction data. Reliable transaction data is the lifeblood of credible financial statements. Unreliable transaction data doomed the Marine Corps audit to failure from the get-go. Without reliable transaction data, the probability of conducting a successful audit of a major component is near zero.

With the right leadership and guidance, a plan with achievable deadlines can and should be developed. In the meantime, we watchdogs—and that is all of us in the Congress of the United States, or at least it ought to be all of us—must remain vigilant. My gut tells me we are still not out of the woods.

I yield the floor.

CONCLUSION OF MORNING BUSINESS

The PRESIDING OFFICER. Morning business is closed.

CYBERSECURITY INFORMATION SHARING ACT OF 2015—MOTION TO PROCEED

The PRESIDING OFFICER. Under the previous order, the Senate will resume consideration of the motion to proceed to S. 754, which the clerk will report.

The legislative clerk read as follows:

Motion to proceed to Calendar No. 28, S. 754, a bill to improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.

Mr. SANDERS. Mr. President, I ask unanimous consent to address the Senate for up to 15 minutes.

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

CAMPAIGN FINANCE REFORM

Mr. SANDERS. Mr. President, on November 19, 1863, standing on the blood-stained battlefield of Gettysburg, Abraham Lincoln delivered one of the most significant and best remembered speeches in American history. At the conclusion of the Gettysburg Address, Lincoln stated ''that we here highly resolve that these dead shall not have died in vain . . . that this nation, under God, shall have a new birth of freedom . . . and that government of the people, by the people, for the people, shall not perish from the earth.''

In the year 2015, with a political campaign finance system that is corrupt and increasingly controlled by billionaires and special interests, I fear very much that, in fact, government of the people, by the people, and for the people is perishing in the United States of America.

Five years ago, in the disastrous Citizens United Supreme Court decision, by a 5-to-4 vote, the U.S. Supreme Court said to the wealthiest people in this country: Billionaires, you already own much of the American economy. Now we are going to give you the opportunity to purchase the U.S. Government, the White House, the U.S. Senate, the U.S. House, Governors' seats, legislatures, and State judicial branches as well. In essence, that is exactly what they said, and, in fact, that is exactly what is happening as we speak.

As a result of Citizens United, during this campaign cycle, billions of dollars from the wealthiest people in this country will flood the political process. Super PACs—a direct outgrowth of the Citizens United decision—enabled the wealthiest people and the largest corporations to contribute unlimited amounts of money to campaigns. According to recent FEC filings, super PACs have raised more than $300 million for the 2016 Presidential election already, and this election cycle has barely begun. This $300 million is more than 11 times what was raised at this point in the 2000 election cycle. What will the situation be 4 years from now? What will the situation be 8 years from now? How many billions and billions of dollars from the wealthy and powerful will be used to elect candidates who represent the rich and the superrich?

According to the Sunlight Foundation, more than $2 out of every $3 raised for Presidential candidates so far is going to super PACs and not to the candidate's own campaign. This is quite extraordinary. What this means is that super PACs, which theoretically operate independently of the actual candidate, have more money and more influence over the candidate's campaign than the candidate himself or herself. Let me repeat that. The millionaires and billionaires who control

the super PACs have more money and more influence over a candidate's campaign than the candidate himself or herself. In other words, the candidate becomes a surrogate, a representative for powerful special interests and is not even in control of his or her own campaign.

Mr. President, 35 individuals or companies have already donated more than $1 million to super PACs so far. According to the Associated Press, almost 60 donors have accounted for nearly one-third of all of the money donated so far in the Presidential race, including donations to the campaigns themselves. Donors giving at least $100,000 account for close to half of all funds raised. Let's be clear. This is all taking place at the early stages of the campaign. We have a long way to go.

We know, for example, that the Koch brothers, worth some $85 billion—the second wealthiest family in America—have made public that they intend to spend some $900 million on this election. This is more money than either the Democratic Party or the Republican Party will spend. One family will be spending more money than either the Democratic Party or the Republican Party. How do we describe a process in which one multibillion-dollar family spends more money on a campaign than either of the two major political parties? Well, I define that process not as democracy but as oligarchy.

Let's be honest and acknowledge what we are talking about. We are talking about a rapid movement in this country toward a political system in which a handful of very wealthy people and special interests will determine who gets elected or who does not get elected. That is not, to say the least, what this country is supposed to be about. That was not, to say the least, the vision of Abraham Lincoln when he talked about a nation in which we had a government of the people, by the people, for the people. That is not what Lincoln's vision was about.

This is not just BERNIE SANDERS expressing a concern. Last week, this is what former President Jimmy Carter had to say about the current campaign finance system on the Thom Hartmann radio show. President Carter stated that unlimited money in politics ''violates the essence of what made America a great country in its political system. Now, it's just an oligarchy, with unlimited political bribery being the essence of getting the nominations for president or to elect the president. And the same thing applies to governors and U.S. Senators and congress members. So now we've just seen a complete subversion of our political system as a payoff to major contributors, who want and expect and sometimes get favors for themselves after the election's over.''

Mr. President, I ask unanimous consent to have President Carter's statement printed in the RECORD.

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

[From the Intercept, July 30, 2015]

JIMMY CARTER: THE U.S. IS AN ''OLIGARCHY WITH UNLIMITED POLITICAL BRIBERY''

(By Jon Schwarz)

Former president Jimmy Carter said Tuesday on the nationally syndicated radio show the Thom Hartmann Program that the United States is now an ''oligarchy'' in which ''unlimited political bribery'' has created ''a complete subversion of our political system as a payoff to major contributors.'' Both Democrats and Republicans, Carter said, ''look upon this unlimited money as a great benefit to themselves.''

Carter was responding to a question from Hartmann about recent Supreme Court decisions on campaign financing like Citizens United.

TRANSCRIPT

HARTMANN: Our Supreme Court has now said, ''unlimited money in politics.'' It seems like a violation of principles of democracy. . . . Your thoughts on that?

CARTER: It violates the essence of what made America a great country in its political system. Now it's just an oligarchy, with unlimited political bribery being the essence of getting the nominations for president or to elect the president. And the same thing applies to governors and U.S. Senators and congress members. So now we've just seen a complete subversion of our political system as a payoff to major contributors, who want and expect and sometimes get favors for themselves after the election's over. . . . The incumbents, Democrats and Republicans, look upon this unlimited money as a great benefit to themselves. Somebody who's already in Congress has a lot more to sell to an avid contributor than somebody who's just a challenger.

Mr. SANDERS. Mr. President, the need for real campaign finance reform is not a progressive issue. It is not a conservative issue. It is an American issue. It is an issue that should concern all Americans, regardless of their political point of view, who wish to preserve the essence of the longest standing democracy in the world, a government which represents all of the people and not a handful of powerful and wealthy special interests.

The need for real campaign finance reform must happen and it must happen as soon as possible. That is why clearly we must overturn, through a constitutional amendment, the disastrous Citizens United Supreme Court decision as well as the Buckley v. Vallejo decision. That is why we need to pass disclosure legislation which will identify all those wealthy individuals who make large campaign contributions. More importantly, it is why we need to move toward public funding of elections.

Our vision for American democracy, our vision for the United States of America, should be a nation in which all people, regardless of their income, can participate in the political process, can run for office without begging for contributions from the wealthy and the powerful. Every Member of the Senate and every Member of the House knows how much time candidates spend on the telephone dialing for dollars—Republicans, Democrats, everybody. This is not what democracy should be about.

Our vision for the future of this country should be one in which candidates are not telling billionaires at special forums what they can do for them. Our vision for democracy should be one in which candidates are speaking to the vast majority of our people—working people, the middle class, low-income people, the elderly, the children, the sick, and the poor—and discussing with them their ideas as to how we can improve lives for all people in this country.

Let us be frank. Let us be honest. The current political campaign finance system is corrupt and amounts to legalized bribery. How can we in the United States tell developing countries how they can go forward in developing their democracies when our system is corrupt? Our vision for the future of this country should be a vision which is inclusive, which tells young people that if you are conservative, if you are progressive, if you are interested in public service, you can run for office without begging the rich and the powerful for campaign contributions.

When Congress returns after the August break, I will be introducing strong legislation which calls for public funding of elections, which will enable any candidate, regardless of his or her political views, to run for office without being beholden to the rich and the powerful. I hope very much the Republican leadership in the Senate will allow this legislation to get to the floor, I hope we can have a serious debate about it, and I hope very much we can go forward to restoring American democracy to a situation in which every citizen of this country has the right to vote and has equal power in determining the future of our great Nation.

Mr. President, with that, I yield the floor.

The PRESIDING OFFICER (Mr. LEE). The Senator from California.

Mrs. FEINSTEIN. Mr. President, I would like to speak in support of the Cybersecurity Information Sharing Act. I had hoped Senator BURR, the chairman of the committee, would be able to deliver the remarks initially. However, he has been unfortunately delayed, and so I will go ahead with my remarks as vice chairman of the committee.

There is no legislative or administrative step we can take that will end all cyber crime and cyber warfare, but as members of the Senate Intelligence Committee, we have heard over the course of several years now that improving the exchange of information and the sharing of that information, company to company and company to the government, can be very helpful and yield a real and significant improvement to cyber security.

Regrettably, this is the third attempt to pass a cyber security information sharing bill. In the almost 5 years that I have been working on this issue, two things have become abundantly clear about passing the bill. First, it must be bipartisan. In 2012, I cosponsored the Lieberman-Collins Cybersecurity Act, which included a title on

information sharing based on a bill I had introduced. It was an important piece of legislation, but it received almost no Republican support and could not gain the 60 votes needed to invoke cloture. It became clear to me then that no cyber security legislation could pass without broad bipartisan support.

The second lesson that has been learned is, it must be narrowly focused. The Lieberman-Collins bill sought to address many critical challenges to our Nation's cyber security. Then-Majority Leader HARRY REID, brought the chairmen of all committees of jurisdiction on our side together and asked them to draft legislation on cyber security in their areas. It soon became clear that addressing so many complex issues makes a bill very difficult to pass. That bill died on the Senate floor in late 2012.

Based on these lessons, we have tried to take a bipartisan and focused approach so Congress can pass a cyber security information sharing bill. In the last Congress, in 2013 and 2014, then-vice chairman of the Intelligence Committee Saxby Chambliss and I sought to draft legislation on information sharing that would attract bipartisan support. We worked through a number of difficult issues together, and we were able to produce a bill that I believed would pass the Senate. The Intelligence Committee approved the bill in 2014 by a strong bipartisan vote of 12 to 3, but it never reached the Senate floor due to privacy concerns about the legislation.

This year, Chairman BURR and I have drafted legislation that both sides can and should support. This bill is bipartisan, it is narrowly focused, and it puts in place a number of privacy protections, many of which I will outline shortly. The bill's bipartisan vote of 14 to 1 in the Senate Intelligence Committee in March underscores this fact.

I would like to thank Senator BURR for his leadership and his willingness to negotiate a bipartisan bill that can and should receive a strong vote. As he often says, neither one of us would have written this bill this way if we were doing it ourselves. This Senator believes it is also true that by negotiating this draft, we will get substantially more votes than either of us can get on our own. I very much hope that is true.

I note that this bill has strong support from the private sector because it creates incentives for improving cyber security and protects companies that take responsible steps to do so. Companies are shielded from lawsuits if they properly use the authorities provided for in this bill. They can be confident that sharing information with other companies or with the government will not subject them to inappropriate regulatory action.

For these reasons, this bill has the support of over 40 business groups, and it is the first bill that has the support of the U.S. Chamber of Commerce. It also has the support of the most important cyber security and critical infrastructure companies in the Nation.

Mr. President, I would like to ask unanimous consent to have those letters printed into the RECORD.

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

AUGUST 3, 2015.

Hon. MITCH MCCONNELL,
U.S. Senate,
Washington, DC.
Hon. HARRY REID,
U.S. Senate,
Washington, DC.

DEAR MAJORITY LEADER MCCONNELL AND MINORITY LEADER REID: On behalf of our diverse members, we write today in strong support of the Cybersecurity Information Sharing Act (S. 754), a bipartisan bill approved earlier this year on a near-unanimous basis by the Select Committee on Intelligence. We strongly urge you to bring up S. 754 as expeditiously as possible, defeat any amendments that would undermine this important legislation, and support the underlying bill.

The threat of cyber-attacks is a real and omnipresent danger to our sector, our members' customers and clients, and to critical infrastructure providers upon which we—and the nation as a whole—rely. S. 754 would enhance our ability to defend the financial services sector and the sensitive data of hundreds of millions of Americans. It is critical that Congress get cybersecurity information sharing legislation to the President's desk before the next crisis, not after.

Our members and the broader financial services industry are dedicated to improving our capacity to protect customers and their sensitive information but as it stands today, our laws do not do enough to foster information sharing and establish clear lines of communication with the various government agencies responsible for cybersecurity. If adopted and signed into law, this legislation will strengthen the nation's ability to defend against cyber-attacks and better protect all Americans by encouraging the business community and the government to quickly and effectively share critical information about these threats while ensuring privacy. More effective information sharing provides some of the strongest protections of privacy, as it is sensitive information from our member firms' customers that we are asking Congress to protect from those who attempt to steal or destroy that information.

Each of our organizations and our respective member firms has made cybersecurity a top priority and we are committed to continuing to work with you and your colleagues in the Senate so that effective cyber threat information sharing legislation can be enacted into law.

Sincerely,

American Bankers Association; American Insurance Association; The Clearing House; Financial Services Institute; Financial Services Roundtable; Investment Company Institute; NACHA—The Electronic Payments Association; The National Association of Mutual Insurance Companies; Property Casualty Insurers Association of America; Securities Industry and Financial Markets Association.

AUGUST 3, 2015.

Hon. MITCH MCCONNELL,
Majority Leader, U.S. Senate,
Washington, DC.
Hon. HARRY REID,
Minority Leader, U.S. Senate,
Washington, DC.

DEAR MAJORITY LEADER MCCONNELL AND MINORITY LEADER REID: The undersigned organizations reiterate their support for cybersecurity information sharing and liability protection legislation and urge the Senate to promptly take up and pass S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015. Enactment of such legislation is urgently needed to further enhance and encourage communication among the federal government, the North American electric power sector, and other critical infrastructure sectors, thus improving our ability to defend against cyber attacks.

While the electric sector already engages in significant information sharing activities and has in place mandatory and enforceable reliability and cybersecurity standards, there remains an urgent need for the government and industry to better share actionable security information in a timely and confidential manner, including protections against public disclosure of sensitive security information. CISA provides a framework to help foster even more meaningful information sharing while maintaining a critical balance between liability and privacy protections.

The electric power sector takes very seriously its responsibility to maintain the reliability, safety, and security of the electric grid. Beyond mandatory standards, the industry maintains an all-hazards ''defense in depth'' mitigation strategy that combines preparation, prevention, resiliency, and response and recovery efforts. We also work closely with the federal government and other critical infrastructure sectors on which the electric sector depends through the Electricity Subsector Coordinating Council, and share electric sector threat information through the Electricity Sector Information Sharing and Analysis Center. Passage of CISA will enhance these activities.

American Public Power Association (APPA); Canadian Electric Association (CEA); Edison Electric Institute (EEI); Electric Power Supply Association (EPSA); GridWise Alliance; Large Public Power Council (LPPC); National Rural Electric Cooperative Association (NRECA); National Association of Regulatory Utility Commissioners (NARUC); Transmission Access Policy Study Group (TAPS).

AMERICAN BANKERS ASSOCIATION,
Washington, DC, August 3, 2015.

Hon. MITCH MCCONNELL,
Majority Leader, U.S. Senate,
Washington, DC.
Hon. RICHARD BURR,
U.S. Senate, Washington, DC.
Hon. HARRY REID,
Minority Leader, U.S. Senate,
Washington, DC.
Hon. DIANNE FEINSTEIN,
U.S. Senate, Washington, DC.

DEAR SENATORS: I am writing on behalf of the members of the American Bankers Association (ABA) to urge you to support the Cybersecurity Information Sharing Act (CISA, S. 754) when it is brought to the Senate floor, and to defeat any amendments that would undermine this critically needed legislation.

CISA is bipartisan legislation introduced by Chairman Richard Burr and Vice Chairman Dianne Feinstein, and reported by a strong bipartisan 14–1 vote in the Senate Intelligence Committee. It will enhance ongoing efforts by the private sector and the Federal government to better protect our critical infrastructure and protect Americans from all walks of life from cyber criminals. Importantly, CISA facilitates increased cyber intelligence information sharing between the private and public sectors, and strikes the appropriate balance between protecting consumer privacy and allowing information sharing on serious threats to our nation's critical infrastructure.

Cybersecurity is a top priority for the financial services industry. Banks invest hundreds of millions of dollars every year to put in place multiple layers of security to protect sensitive data. Protecting customers has always been and will remain our top priority and CISA will help us work more effectively with the Federal government and other sectors of the economy to better protect them from cyber attacks.

We urge you to support this important legislation and pass it as soon as possible to better protect America's cybersecurity infrastructure against current and future threats.

Sincerely,

JAMES C. BALLENTINE.

INFORMATION TECHNOLOGY INDUSTRY COUNCIL,
Washington, DC, July 23, 2015.

Hon. MITCH MCCONNELL,
Majority Leader, U.S. Senate,
Washington, DC.
Hon. HARRY REID,
Democratic Leader, U.S. Senate,
Washington, DC.

DEAR MAJORITY LEADER MCCONNELL AND DEMOCRATIC LEADER REID: On behalf of the members of the Information Technology Industry Council (ITI), I write to express our support for S. 754, the Cybersecurity Information Sharing Act of 2015 (CISA), and urge you to bring it to the Senate floor for debate and vote. Given the importance of cybersecurity threat information sharing to the high-tech industry, we will consider scoring votes in support of CISA in our 114th Congressional Voting Guide.

ITI members contribute to making the U.S. information and communication technology (ICT) industry the strongest in the world in innovative cybersecurity practices and solutions. We firmly believe that passing legislation to help increase voluntary cybersecurity threat information sharing between the private sector and the federal government, and within the private sector, is an important step Congress can take to enable all stakeholders to address threats, stem losses, and shield their systems, partners and customers. It is important that the Senate act now to pass CISA and continue to move the legislative process forward, so that Congress can reconcile CISA with the House cybersecurity legislation, H.R. 1560, the Protecting Cyber Networks Act, and H.R. 1731, the National Cybersecurity Protection Advancement Act of 2015, and send a bill to the president.

ITI believes that legislation to promote greater cybersecurity threat information sharing should:

Affirm that cybersecurity threat information sharing be voluntary;

Promote multidirectional cybersecurity threat information sharing, allowing private-to-private, private-to-government and government-to-private sharing relationships;

Include targeted liability protections;

Utilize a civilian agency interface for private-to-government information sharing to which new liability protections attach;

Promote technology-neutral mechanisms that enable cybersecurity threat information to be shared in as close to real-time as possible;

Require all entities to take reasonable steps to remove personally identifiable information from information shared through data minimization; and

Ensure private sector use of information received through private-to-private sharing is only for cybersecurity purposes, and government use of information received from the private sector is limited to cybersecurity purposes and used by law enforcement only:

For the investigation and prosecution of cyber crimes;

For the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger; and

For the protection of minors from child pornography.

We appreciate the progress made by the Senate Intelligence Committee to include provisions that would protect personally identifiable information while also allowing for a cybersecurity threat information sharing framework that will enhance our ability to protect and defend our networks.

We look forward to working closely with you, your committee leadership, and the House of Representatives to further address outstanding issues in conference to ensure it adheres to our above cybersecurity threat information sharing principles. ITI remains committed to refining the legislation and supporting a final product that can best achieve our goal of promoting greater cybersecurity.

Sincerely,

DEAN C. GARFIELD,
President & CEO.

BSA/THE SOFTWARE ALLIANCE,
Washington, DC, July 21, 2015.

Hon. MITCH MCCONNELL,
Senate Majority Leader,
Washington, DC.
Hon. HARRY REID,
Senate Minority Leader,
Washington, DC.

DEAR MAJORITY LEADER MCCONNELL AND MINORITY LEADER REID: On behalf of BSA/The Software Alliance, I write in support of bringing the Cybersecurity Information Sharing Act of 2015 (S. 754) to the Senate floor for a robust debate. Enactment of bipartisan legislation that enhances voluntary cyber threat information sharing while ensuring privacy protection will be an important step in bolstering our nation's cybersecurity capabilities.

Our members are on the front lines defending against cyber attacks. Every day, bad actors are attacking networks to extract valuable private and commercial information. We believe it is now more important than ever to enact legislation to break down the legal barriers that currently discourage cyber threat information sharing between and among the public and private sectors. Increased awareness will enhance the ability of businesses, consumers, and critical infrastructure to better defend themselves against attacks and intrusions. We are confident that all of these goals can be accomplished without comprising the privacy of an individual's information.

I appreciate your leadership on moving this important legislation forward to a successful outcome in the Senate. We support this bipartisan effort and look forward to working with you in the process to ultimately move a cyber threat information sharing bill to the President's desk for signature.

Sincerely,

VICTORIA A. ESPINEL,
President and CEO.

PROTECTING AMERICA'S CYBER NETWORKS COALITION,
July 21, 2015.

TO THE MEMBERS OF THE UNITED STATES SENATE: The Protecting America's Cyber Networks Coalition (the coalition) urges the Senate to take up and pass S. 754, the Cybersecurity Information Sharing Act (CISA) of 2015. Passing cybersecurity information-sharing legislation is a top policy priority of the coalition, which is a partnership of leading business associations representing nearly every sector of the U.S. economy.

In March, the Select Committee on Intelligence passed CISA by a strong bipartisan vote (14–1). The Senate can build on the momentum generated in the House to move CISA forward. In April, the House passed two cybersecurity information-sharing bills—H.R. 1560, the Protecting Cyber Networks Act (PCNA), and H.R. 1731, the National Cybersecurity Protection Advancement Act (NCPAA) of 2015—with robust majorities from both parties and broad industry support.

Our organizations believe that Congress needs to send a bill to the president that gives businesses legal certainty that they have safe harbor against frivolous lawsuits when voluntarily sharing and receiving threat indicators and defensive measures in real time and taking actions to mitigate cyberattacks.

The legislation also needs to offer protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities. Coalition members also believe that legislation needs to safeguard privacy and civil liberties and establish appropriate roles for government agencies and departments. CISA reflects sound compromises among many stakeholders on these issues.

Recent cyber incidents underscore the need for legislation to help businesses improve their awareness of cyber threats and to enhance their protection and response capabilities in collaboration with government entities. Cyberattacks aimed at U.S. businesses and government bodies are increasingly being launched from sophisticated hackers, organized crime, and state-sponsored groups. These attacks are advancing in scope and complexity.

The coalition is committed to working with lawmakers and their staff members to get cybersecurity information-sharing legislation quickly enacted to strengthen our national security and the protection and resilience of U.S. industry. Congressional action cannot come soon enough.

Sincerely,

Agricultural Retailers Association (ARA); Airlines for America (A4A); Alliance of Automobile Manufacturers; American Bankers Association (ABA); American Cable Association (ACA); American Council of Life Insurers (ACLI); American Fuel & Petrochemical Manufacturers (AFPM); American Gaming Association; American Gas Association (AGA); American Insurance Association (AIA); American Petroleum Institute (API); American Public Power Association (APPA); American Water Works Association (AWWA); ASIS International; Association of American Railroads (AAR); BITS—Financial Services Roundtable; College of Healthcare Information Management Executives (CHIME); CompTIA—The Computing Technology Industry Association; CTIA—The Wireless Association; Edison Electric Institute (EEI); Federation of American Hospitals (FAH); Food Marketing Institute (FMI).

GridWise Alliance; HIMSS—Healthcare Information and Management Systems Society; HITRUST—Health Information Trust Alliance; Large Public Power Council (LPPC); National Association of Chemical Distributors (NACD); National Association of Manufacturers (NAM); National Association of Mutual Insurance Companies (NAMIC); National Association of Water Companies (NAWC); National Business Coalition on e-Commerce & Privacy; National Cable & Telecommunications Association (NCTA); National Rural Electric Cooperative Association (NRECA).

NTCA—The Rural Broadband Association; Property Casualty Insurers Association of America (PCI); The Real Estate Roundtable; Securities Industry and Financial Markets Association (SIFMA); Society of Chemical Manufacturers & Affiliates (SOCMA); Telecommunications Industry Association (TIA); Transmission Access Policy Study Group (TAPS); United States Telecom Association (USTelecom);

U.S. Chamber of Commerce; Utilities Telecom Council (UTC).

CHAMBER OF COMMERCE OF
THE UNITED STATES OF AMERICA,
February 14, 2015.

TO THE MEMBERS OF THE UNITED STATES SENATE: As the Senate prepares to consider S. 754, the ''Cybersecurity Information Sharing Act of 2015,'' the U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than three million businesses of all sizes, sectors, and regions, as well as state and local chambers and industry associations, and dedicated to promoting, protecting, and defending America's free enterprise system, writes to express our strong opposition to the adoption of amendments that would weaken or overly complicate this important bipartisan bill, including issues related to data security, breach notification, or commercial privacy, which are best addressed in other contexts.

The Chamber believes that all provisions of S. 754 must support the important goal of protecting critical infrastructure. Unrelated issues, such as data security, breach notification, and commercial privacy legislation, have not yet received any consideration in the committees of jurisdiction and are not ready for consideration by the full Senate. These sensitive topics should proceed through the legislative process following regular order to ensure complete and deliberate consideration separate from the pending floor debate on cybersecurity information sharing legislation.

Cybersecurity information sharing legislation meets a dire national security need, and though the Chamber would like to see meaningful data security, breach notification, and commercial privacy legislation become law, for the benefit of businesses and consumers alike, we are equally steadfast in our belief that cybersecurity information sharing legislation is important for national security and should be Congress's immediate priority.

There are 47 separate state laws which deal directly with data security and breach notification. The business community has been working with members of Congress in both chambers and on both sides of the aisle to find the right path toward passage of a national data security and breach notification law. However, much work remains to be done, as disagreement continues regarding certain provisions which would be contained in federal legislation. This disagreement is evident in virtually every one of the significantly different data security bills which have been introduced in the Senate during the last several Congresses.

The Chamber has appreciated the opportunity to comment on and offer edits to the various bills and looks forward to working with their authors and cosponsors as legislation works its way through the committee process. However, data security legislation deserves its own due consideration and deliberate debate, separate from the complicated and pressing national security issue of cybersecurity information sharing. For example, the House Energy and Commerce committee has held multiple hearings on proposed legislation in addition to a subcommittee markup and planned mark up at the full committee level. Though there are issues which need to be resolved in that legislation, the Chamber appreciates the process and consideration given and that the bill has worked its way through the proper channels.

Given the work that still needs to be done on data security proposals, the Chamber urges you to keep them separate and apart from cybersecurity information sharing legislation and not rush to make changes to the current landscape of state data security, data breach, and commercial privacy laws. Doing so would have a fundamentally negative impact on a broad segment of the American business community.

Sincerely,

R. BRUCE JOSTEN.

Mrs. FEINSTEIN. At the same time, the bill includes numerous privacy protections beyond those contained in last year's bill. Senator BURR and I worked together to address the specific concerns raised by the administration, some of our Senate colleagues, and other key stakeholders. Because of these changes, the administration said yesterday that ''cyber security is an important national security issue and the Senate should take up this bill as soon as possible and pass it.''

I believe this is a good bill and will allow companies and the government to improve the security of their computer networks, but this is just a first-step bill. It will not bring an end to successful cyber attacks or thefts, but it will help to address the problem.

What does this bill do? It provides clear direction for the government to share cyber threat information and defensive measures with the private sector.

Two, it authorizes private companies to monitor their computer networks and to share cyber threat information and defensive measures with other companies and with the Federal, State, local, and tribal government.

And three, it creates a process and rules to limit how the Federal Government will and will not use the information it receives.

Companies are granted liability protection for the appropriate monitoring for cyber threats and for sharing and receiving cyber threat information. This liability protection exists for both company-to-company sharing as well as company-to-government sharing consistent with the bill's terms. Companies are also authorized to use defensive measures on their own networks for cyber security purposes.

Since the bill is complicated, let me describe what the bill does in more detail.

First, it recognizes that the Federal Government has information about cyber threats that it can and should share with the private sector and with State, local, and tribal governments. The bill requires the Director of National Intelligence to put in place a process that will increase the sharing of information on cyber threats already in the government's hands with the private sector and help protect an individual or a business.

Importantly, as the first order of business, there will be a managers' amendment which makes changes to specifically limit the ways the government can use the cyber security information it receives. This amendment was distributed on Friday. I would urge everyone to look at it because under the amendment, this bill can only be used for cyber security purposes—no others. It is not a surveillance bill; it is strictly related to cyber security. The bill previously allowed the government to use the information to investigate and prosecute serious violent felonies. That has drawn substantial opposition, and we have removed it in the managers' package.

I would now like to take a minute to go over some of the privacy protections in the bill.

No. 1, the bill is strictly voluntary. It does not require companies to do anything they choose not to do. There is no requirement to share information with another company or with the government. The government cannot compel any sharing by the private sector. It is completely voluntary.

No. 2, it narrowly defines the term ''cyber threat indicator'' to limit the amount of information that may be shared under the bill. Companies do not share information under this bill unless it is specifically about a cyber threat or a cyber defense—nothing else.

No. 3, the authorizations are clear but limited. Companies are fully authorized to do three things: monitor their networks or provide monitoring services to their customers to identify cyber threats; use limited defensive measures to protect against cyber threats on their networks; and to share and receive information with each other and with Federal, State, and local governments.

No. 4, there are mandatory steps companies must take, before sharing any cyber threat information with other companies or the government, to review the information for irrelevant privacy information. In other words, the companies must do a privacy scrub. They are required to remove any personal information that is found. Companies cannot, as it has been alleged, simply hand over customer information.

No. 5, the bill requires that the Attorney General establish mandatory guidelines to protect privacy for any information the government receives. These guidelines will be public, and they will include consultation with the private sector prior to them being put together.

The bill requires them to limit how long the government can retain any information and provide notification and a process to destroy mistakenly shared information. It also requires the Attorney General to create sanctions for any government official who does not follow these mandatory privacy guidelines.

No. 6, the Department of Homeland Security, not the Department of Defense or the intelligence community, is the primary recipient of cyber information. In the managers' amendment, we strengthen the role the Secretary of Homeland Security has in deciding how information sharing will take place.

No. 7, once the managers' amendment is adopted, the bill will restrict the government's use of voluntarily shared information, so the government cannot use this information for law enforcement purposes unrelated to cyber security and cyber crime.

No. 8, the bill limits liability protections to monitoring for cyber threats and sharing information about them and only—and only—if a company complies with the bill's privacy requirements. The bill explicitly excludes protection for gross negligence or willful misconduct.

No. 9, above and beyond these mandatory protections, there are a number of oversight mechanisms in the bill, including reports by heads of agencies, inspectors general, and the Privacy and Civil Liberties Oversight Board.

In sum, this bill allows for strictly voluntary sharing of cyber security information and many layers of privacy protection.

It is my understanding that the chairman of our committee is here, so I would like to skip to the conclusion of my remarks and then be able to turn this over to him.

The House of Representatives has already passed two bills this year to improve cyber security information sharing. The Intelligence Committee has crafted a carefully balanced bill that passed by a 14-to-1 vote in March and it has improved significantly since then through the managers' amendment.

We very much need to take this first step on cyber security to address the almost daily reports of hacking and cyber threats. I very much hope the Senate will take action now.

Now I will yield the floor. I want to thank the chairman. It has been a pleasure, Mr. Chairman, to work with you. I think I speak for every member of the committee. I am very pleased we have this bill on the floor. God willing and the Members willing, we will be able to pass it one day.

I yield the floor to the chair of the Intelligence Committee.

The PRESIDING OFFICER. The Senator from North Carolina.

Mr. BURR. Mr. President, I want to thank my good friend and vice chair of the Intelligence Committee, Senator FEINSTEIN. She has been in the trenches working on cyber security legislation longer than I have. Her passion is displayed in the product that has come out. There has been no person more outspoken on privacy than DIANNE FEINSTEIN. There is no person who has been more outspoken on the need for us to get this right than Senator FEINSTEIN.

Daily, she and I look at some of the most sensitive intelligence information that exists in this country. We are charged as a committee—15 individuals out of a body of 100—to provide the oversight to an intelligence community to make sure they live within the letters of the law or the boundaries set by Executive order. Every day we try to fulfill that job.

We are sometimes tasked with producing legislation, and that is why we are here today with the cyber security bill. It has been referred to that we are here because OPM got hacked. No. We are here because the American people's data will be in jeopardy if government does not help to find a way to help minimize the loss.

So where is the threat? The threat is to business, it is to government, and it is to individuals. There is no part of America that is left out of this. The legislation we are proposing affects everybody in this country—big and small business, State and Federal governments, and individuals, no matter where they live or how much they are worth. I think it is safe to say today that business and government have both been attacked, they have been penetrated, and data has been lost. In some cases that intent was criminal; in some cases the intent was nation-states. It was towards credit cards on one side or Social Security numbers, and on the other side it was plans for the next military platform or intellectual property that was owned by a company. But we are where we are, and now we have a proposal as to how we minimize.

Let me emphasize this. You heard it from the vice chairman. This bill does not prevent cyber attacks. I am not sure that we could craft anything that would do that. What this bill does is for the first time it allows us a pathway to minimizing the amount of data that is lost and for the first time empowering government, once they get the pertinent information, to push out to the rest of business and to individuals and to governments: Here is the type of attack that is happening. Here is the tool they are using. Here is the defensive mechanism you can put on your system that will provide you comfort that they cannot penetrate you and provide the company that has been attacked comfort that it might be able to minimize in real time the amount of data that is lost.

So, as the vice chairman said, these are key points on this piece of legislation: It is voluntary. There is no entity in America that is forced to report. It is a purely voluntary system. To have participation in a voluntary system, you have to listen to the folks who are the subjects of these attacks as to what they need to act in real time and to provide pertinent data.

It is an information-sharing bill. It is not a surveillance bill. I say to those who have characterized it that way that we have done everything we can to clarify with the managers' amendment that there is no surveillance. The only thing we are after is minimizing the loss of data that exists.

Here is how it works. I want to break it into three categories.

This bill covers private to private. It says that if I am a private company and my IT system gets hacked and I get penetrated, I can automatically pick up the phone and call the IT people at my competitor's business, and I am protected under antitrust, that we can carry out a conversation so that I can figure out whether they got hacked, and if they did but they did not get penetrated, what software did they have on their system that secured their data. I can immediately go and put that on my system, and I can minimize the loss of any additional data. So we protect for that private-to-private conversation only for the purposes of sharing cyber information.

We also have private to government. We allow any company, in real time—at the same time they are talking to a competitor, they can transmit electronically the pertinent data that it takes to do the forensics of what happened. What tool did they use? They can transfer that to government, and they are protected from a liability standpoint for the transfer of that—the vice chairman got into all of this, so I do not want to rehash it—with the correct protections of personal data. The company is required not to send personal data. Any government agency that is the recipient of this data, as they go through it, if they see personal data that is not relevant to the determination of what type of attack, what type of tool, what type of response, then they have to minimize that data so it is not released.

In addition, we have government to private, which is the third leg. It amazed me that the government did not have the authority to push out a lot of information. What we do is we empower the government to analyze the attack, to determine the tool that was used, to find the most appropriate defensive software mechanism, and then to say to business broadly: There is an attack that has happened in America. This is the tool they used. This is the defensive mechanism that will protect the data at your company.

If you ask me, I think this is what we are here for. This is what the Congress of the United States is supposed to do—facilitate, through minor tweaks, a voluntary participation to close the door and minimize potential loss. That is all we are attempting to do.

I want to loop back to where the vice chairman was. We are now at the point where we are asking our colleagues for unanimous consent to come to the floor and actually take up this bill. Moving to the bill allows our colleagues to come to the floor with relevant amendments to the bill, where they can be debated and voted on.

I actually believe, Vice Chairman, if we could do that now, we could process this entire bill and all of the amendments that are relevant by this time tomorrow. That would mean we would have to work and we would have to talk and we would have to vote, but we could do it because I think when we look at the array of relevant amendments, they are pretty well defined. Some of them are duplications of others that people have planned to talk about.

But to suggest that this is a problem, which it is—we have seen it with over 22 million government workers whose personal data and in some cases, because of the forms they had to fill out for security clearance, their most sensitive data has gotten out of the OPM system.

Just because OPM was the last one, don't think that somebody wasn't serious. Don't think that Anthem Blue Cross wasn't serious. Don't think that some of the attacks that only acquired credit card information aren't serious.

What we are attempting to do is to minimize the degree of that loss. All we need is the cooperation of every Member of the Senate to say: I am willing to move to the bill. I am willing to bring up amendments—relevant amendments—willing to debate them and willing to vote on them.

Process is where we are. At the end of the day, we can determine whether this is a bill that is worthy to move on. It is not the end of the road because once we get through in the Senate we have to conference the bill with the House of Representatives. As the vice chairman pointed out, they have produced multiple pieces of legislation. It is the Senate that is now holding us back.

I urge my colleagues: Let's agree to move to the bill. Let's agree to relevant amendments, and let's process this cyber security bill so that when we come back from August, we can actually sit down with our colleagues in the House, conference a bill, and provide the American people with a little bit of security, knowing that we are going to minimize the amount of data that is lost, because of a voluntary program between the private sector and the government.

I think the vice chairman shares my belief that we are not scared to have a debate on relevant amendments on this bill. We understand there are more views than just ours. But we have to get on the bill to be able to offer amendments, to be able to share what we know that might not necessarily support the amendment.

Right now, we are sort of frozen because we cannot offer amendments, including the managers' amendment, which I would say to my colleagues—and the vice chairman said this in a very specific way—if you will read the managers' amendment, a lot of the concerns that people have will vanish. Nobody will call it a surveillance bill because we have addressed the issues that people were concerned with. Although we didn't think they were problems before, we clarified it in a way that it is limited only to cyber security. I could make a tremendous case that through the cyber security forensic process, if we found another criminal act, the American people probably would want that reported—without a doubt.

Mr. MCCAIN. Will the Senator yield for a question?

Mr. BURR. I am pleased to yield for a question.

Mr. MCCAIN. In light of recent events that have dominated the news, including the breach of millions of Americans' privileged information, which could be used in ways to harm them, do you think it is a good idea for the Senate to go out into a month-long recess without at least having debates, votes, and amendments on this issue?

Does the Senator know of an issue right now that impacts the lives of everyday Americans such as this threat of cyber security attacks on the citizens of the United States?

Mr. BURR. I thank the Senator for the question, and I think he knows the answer.

We should dispose of this. The easiest way, as I shared earlier, is that if we get on this bill and we process amendments, if we really wanted to, we could finish tomorrow. The reality is that it doesn't take a long time to debate amendments, to vote on amendments, and to be done.

At the end of the day, every Member would have to make a decision as to whether they are supportive or against the bill. But not getting on the bill, not offering amendments cheats the American people.

Mr. MCCAIN. I will just ask one more question.

It is obvious that the Senator from California and the Senator from North Carolina have worked very closely together on this issue. They are the two leaders on intelligence now for a number of years.

Wouldn't it seem logical that with a bipartisan piece of legislation that addresses an issue—I guess my question is this: How many Americans have been affected most recently by cyber attacks, and what would this legislation do to try to prohibit that from happening again? Don't we have some obligation to try to address the vulnerabilities of average American everyday citizens?

Mr. BURR. I think the answer is there have been millions of Americans whose private data has been breached for numerous reasons. The Senator from Arizona is correct. We have an obligation to do what we can to minimize that loss.

Mr. MCCAIN. And isn't this a bipartisan product?

Mr. BURR. Well, this is very much a bipartisan bill, and I think it is a bicameral effort. It is not as if this is a limb we are walking out on and the House isn't already out there. Emphatically, I implore my colleagues: Let's get on the bill. Let's come and offer relevant amendments, and let's process those amendments as quickly as we can. I think we can accommodate both, the need to leave for August and to go see the people we are married to and get away from the people we see every day who influence us in numerous ways—I am speaking of the Senator from Arizona right now, and I know he is anxious to go somewhere other than here—and to process this bill, which is to do our work. To not get on the bill, to not offer amendments is to ignore the responsibilities that we have.

Mr. MCCAIN. I wish to just finally say to the Senator from North Carolina that I appreciate the hard work he and the Senator from California have put in on this issue. It has been said by our military leaders that right now one of the greatest vulnerabilities to national security is the possibility or likelihood of cyber attacks. The implications of that far exceed that of the invasion of someone's privacy.

I thank him and the Senator from California for their hard work on this. I think it at least deserves debate and amendments, and hopefully we can pass it before we go out for the recess.

Mr. BURR. I thank the Senator from Arizona, who has worked closely with us since the beginning to try to move this bill together. Hopefully, at our lunches today, we will have an opportunity to talk to our Members in the hopes that we can come back from lunch and maybe get started on this bill.

With that, I yield the floor.

The PRESIDING OFFICER. The Senator from Virginia.

Mr. KAINE. Mr. President, I ask unanimous consent to speak for up to 10 minutes, recognizing that it is after 12:30 p.m.

The PRESIDING OFFICER. Is there objection?

Without objection, it is so ordered.

NUCLEAR AGREEMENT WITH IRAN

Mr. KAINE. Mr. President, in November 2013, the United States and five global powers, the P5+1, announced an interim deal to freeze Iran's nuclear program and negotiate a diplomatic resolution to one of the most challenging issues affecting global security.

Since then, as a member of the Senate Armed Services Committee and the Foreign Relations Committee, I participated in scores of hearings, classified briefings, meetings, and calls about this topic in Virginia, Washington, and during five trips to the Middle East, including two trips to Israel.

I have listened to the administration, to allies in the Middle East and elsewhere, to current and former Senate colleagues—especially former Armed Services Chairmen John Warner and Carl Levin—to national security and foreign policy experts, to critics and proponents of the deal, to American military leaders and troops, and also to my constituents. I helped write the Iran Nuclear Agreement Review Act, under which Congress is currently engaging in a 60-day review period to approve or disapprove of the suspension of congressional sanctions as part of the final deal announced July 15.

Based on my review of this complex matter, I acknowledge that every option before us involves risk with upside and downside consequences.

I understand how people of good will can reach different conclusions, but I also conclude that the Joint Comprehensive Plan of Action is a dramatic improvement over the status quo at improving global security for the next 15 years and, likely, longer.

In this deal, America has honored its best traditions and shown that patient

diplomacy can achieve what isolation and hostility cannot.

For this reason, I will support the deal.

Prior to the interim negotiation in November of 2013, and even in the face of a punishing international sanctions regime, Iran's nuclear program was marching ahead. Iran had amassed more than 19,000 centrifuges to enrich uranium, and that number was growing. Iran had produced more than 11,000 kilograms of enriched uranium, and that stockpile was growing. Iran had perfected the ability to enrich uranium to the 20-percent level, and that enrichment level was growing. Iran was constructing a heavy-water facility at Arak capable of producing weapons-grade plutonium, and Iran only allowed limited IAEA access to its declared nuclear facilities, shielding its operation and inspection of covert nuclear sites.

The program, when diplomacy began, was months away from being able to produce enough enriched uranium to make a nuclear weapon.

Israeli Prime Minister Benjamin Netanyahu told the United Nations in 2012:

> For over seven years, the international community has tried sanctions with Iran. Under the leadership of President Obama, the international community has passed some of the strongest sanctions to date. . . . It's had an effect on the economy, but we must face the truth. Sanctions have not stopped Iran's nuclear program.

We must face the truth. A punishing sanctions regime did not stop Iran's nuclear program. The nuclear program will only stop by a diplomatic agreement or by military action. While military action has to be an option, it is in America's interest—and in the interest of the entire world—to use every effort to find a diplomatic resolution. In fact, that was the purpose of the Iranian sanctions to begin with—to open a path to a diplomatic solution.

We now have a diplomatic solution on the table. The JCPOA is not perfect because all parties made concessions, as is the case in any serious diplomatic negotiation. But it has gained broad international support because it prevents Iran from getting sufficient uranium for a bomb for at least 15 years. It also stops any pathway to a plutonium weapon for that period, and it exposes Iranian covert activity to enhanced scrutiny by the international community forever.

Under the deal, Iran does the following: It affirms that ''under no circumstances will Iran ever seek, develop or acquire any nuclear weapons,'' it reduces its quantity of centrifuges by more than two-thirds, and it slashes its uranium stockpile by 97 percent to 300 kilograms for 15 years. This is dramatically less than what Iran would need to produce even a single weapon. It caps the enrichment level of the remaining uranium stockpile at 3.67 percent. It reconfigures the Iraq reactor so that it can no longer produce weapons-grade plutonium. It commits to a series of limitations on R&D activities to guarantee that any nuclear program will be ''for exclusively peaceful purposes'' in full compliance with international nonproliferation rules. Finally, Iran agrees to a robust set of international inspections of its declared nuclear facilities, its entire uranium supply chain, and its suspected covert facilities by a team of more than 130 international inspectors.

After year 15, the unique caps and requirements imposed on Iran are progressively lifted through year 2025. After year 25, Iran is permanently obligated to abide by all international nonproliferation treaty requirements, including the extensive inspections required by the NPT Additional Protocol, and its agreement that it will never ''seek, develop, or acquire any nuclear weapons'' continues forever.

If Iran breaks this agreement, nuclear sanctions may be reimposed. The United States reserves the right to sanction Iran for activities unrelated to its nuclear program, including support for terrorism, arms shipments, and human rights violations.

Finally, and importantly, the United States and our partners maintain the ability to use military action if Iran seeks to obtain a nuclear weapon in violation of this deal. The knowledge of the Iranian program gained through extensive inspections will improve the effectiveness of any military action, and the clarity of Iran's commitment to the world—in the first paragraph of the agreement—that it will never pursue nuclear weapons will make it easier to gain international support for military action should Iran violate their unequivocal pledge.

This deal does not solve all outstanding issues with an adversarial regime. In that sense, it is similar to the Nuclear Test Ban Treaty President Kennedy negotiated with the Soviet Union in the midst of the Cold War. Iran's support for terrorism remains a major concern, and we must increase efforts with our regional allies to counter those malign activities. But at the end of the day, this agreement is not about making an ally out of an adversary, it is about denying an adversary a path to obtaining nuclear weapons.

This deal takes a nuclear weapons program that was on the verge of success and disables it for many years through peaceful diplomatic means with sufficient tools for the international community to verify whether Iran is meeting its commitments. I hope this resolution might open the door to diplomatic discussion of other tough issues with Iran.

In conclusion, monitoring this agreement and countering Iran's nonnuclear activity will require great diligence by the United States, our allies, and the IAEA, and there will be an important role for Congress in this ongoing work. I look forward to working with my colleagues on measures to guarantee close supervision and enforcement of this deal. That work will be arduous, but it is far preferable to allowing Iran to return to a march toward nuclear weapons. It is also far preferable to any other alternative, including war.

Mr. President, I yield the floor.

RECESS

The PRESIDING OFFICER. Under the previous order, the Senate stands in recess until 2:15 p.m. today.

Thereupon, the Senate, at 12:46 p.m., recessed until 2:15 p.m. and reassembled when called to order by the Presiding Officer (Mr. PORTMAN).

CYBERSECURITY INFORMATION SHARING ACT OF 2015—MOTION TO PROCEED—Continued

The PRESIDING OFFICER. The Senator from Arizona.

Mr. MCCAIN. Mr. President, I would like to thank my friend from Florida, Senator NELSON, for allowing me to speak for 5 minutes. I ask unanimous consent that he be recognized immediately following me—not the Senator from New Mexico, the Senator from Florida.

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

Mr. MCCAIN. Mr. President, I rise in strong support of S. 754, the Cybersecurity Information Sharing Act. I want to thank my colleagues Chairman BURR and Vice Chairman FEINSTEIN for their leadership on this critically important legislation. This bill, 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.

Enacting legislation to confront the accumulating dangers of cyber threats must be among the highest national security priorities of the Congress. Cyber attacks on our Nation have become disturbingly common. More recently, it was the Office of Personnel Management. A few weeks before that, it was the Pentagon network, the White House, and the State Department. Before that it was Anthem and Sony—just to name a few. The status quo is unacceptable, and Congress needs to do its part in passing this legislation. But the President, as our Nation's Commander in Chief, must also do his part to deter the belligerence of our adversaries in cyber space.

The threats from China, Russia, North Korea, and Iran—not to mention the aspirations of terrorist organizations like ISIL and Al Qaeda—are steadily growing in number and severity. And our national security leadership has warned us repeatedly that we could face a cyber attack against our Nation's critical infrastructure in the not too distant future. I believe our response to such an attack, or lack thereof, could define the future of warfare.

To date, the U.S. response to cyber attacks has been tepid at best, and nonexistent at worst. Unless and until